S01P1295 US0(

J1000 U.S. PTO
09/941899
08/29/01

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年 ８月３１日

出願番号
Application Number: 特願２０００－２６４５１５

出願人
Applicant(s): ソニー株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２００１年 ５月２５日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願

【整理番号】　00004645

【提出日】　平成12年 8月31日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 15/00

【発明の名称】　個人識別証明書リンクシステム、情報処理装置、および情報処理方法、並びにプログラム提供媒体

【請求項の数】　15

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　昆　雅士

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　石橋　義人

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　松山　科子

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　二村　一郎

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　渡辺　秀明

出証特２００１－３０４４８１６

【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代表者】　出井　伸之
【代理人】
【識別番号】　100101801
【弁理士】
【氏名又は名称】　山田　英治
【電話番号】　03-5541-7577
【選任した代理人】
【識別番号】　100093241
【弁理士】
【氏名又は名称】　宮田　正昭
【電話番号】　03-5541-7577
【選任した代理人】
【識別番号】　100086531
【弁理士】
【氏名又は名称】　澤田　俊夫
【電話番号】　03-5541-7577
【手数料の表示】
【予納台帳番号】　062721
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9904833
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　個人識別証明書リンクシステム、情報処理装置、および情報処理方法、並びにプログラム提供媒体

【特許請求の範囲】

【請求項１】

暗号処理鍵である公開鍵を格納し、認証局が生成する公開鍵証明書と、個人識別データであるテンプレートを格納し、個人識別認証局が生成する個人識別証明書との間で、２以上の証明書を関連づけたリンクを形成し、１つの証明書に基づいて他の関連証明書を特定可能とした構成を有することを特徴とする個人識別証明書リンクシステム。

【請求項２】

前記証明書のリンクは、

個人識別証明書と、

該個人識別証明書の格納テンプレートの暗号化に適用した公開鍵の公開鍵証明書とを関連付けたリンクであることを特徴とする請求項１に記載の個人識別証明書リンクシステム。

【請求項３】

前記証明書のリンクは、

データ通信先との接続処理の際に適用する個人識別証明書と公開鍵証明書との組合わせを関連付けたリンクであることを特徴とする請求項１に記載の個人識別証明書リンクシステム。

【請求項４】

前記公開鍵証明書または前記個人識別証明書は、リンクを持つ異なる証明書の識別子をデータとして格納した構成であることを特徴とする請求項１に記載の個人識別証明書リンクシステム。

【請求項５】

前記公開鍵証明書または前記個人識別証明書は、リンク識別データとしてのリンク構造体識別子と、リンクを構成する公開鍵証明書識別子と、個人識別証明書識別子とをデータとして格納した構成であることを特徴とする請求項１に記載の

個人識別証明書リンクシステム。

【請求項６】

リンクを構成する公開鍵証明書の識別子と、個人識別証明書との識別子との組データを格納した組情報を、各証明書と別のデータとして構成し管理する構成としたことを特徴とする請求項１に記載の個人識別証明書リンクシステム。

【請求項７】

リンクを構成する公開鍵証明書の識別子と、個人識別証明書との識別子との組データを格納した組情報を、各証明書と別のデータとして構成し管理し、さらに、

前記組情報を一次情報として、前記組情報に関連する二次情報を前記一次情報から特定可能としたリンクを形成したことを特徴とする請求項１に記載の個人識別証明書リンクシステム。

【請求項８】

前記公開鍵証明書または前記個人識別証明書は、リンクを持つ異なる証明書を格納した構成であることを特徴とする請求項１に記載の個人識別証明書リンクシステム。

【請求項９】

前記認証局、前記個人識別認証局は、公開鍵証明書および個人識別証明書の利用当時者以外の第三者機関として構成されていることを特徴とする請求項１に記載の個人識別証明書リンクシステム。

【請求項１０】

予め取得した個人識別データであるテンプレートと、ユーザの入力したサンプリング情報との照合により個人認証を実行する情報処理装置において、

前記テンプレートを含むテンプレート情報を暗号化して格納し、第三者機関である個人識別認証局が生成した個人識別証明書から暗号化テンプレートを取得するとともに、該個人識別証明書に格納されたリンク情報に従って公開鍵証明書を特定し、該特定された公開鍵証明書に基づいてテンプレートの暗号処理鍵を特定し、テンプレートの暗号化または復号処理を実行する構成を有することを特徴とする情報処理装置。

【請求項１１】

予め取得した個人識別データであるテンプレートと、ユーザの入力したサンプリング情報との照合により個人認証を実行する情報処理装置において、

第三者機関である個人識別認証局が生成した個人識別証明書から暗号化テンプレートを取得し、テンプレートに基づいて個人認証処理を実行するとともに、

該個人識別証明書に格納されたリンク情報に従って公開鍵証明書を特定し、該特定された公開鍵証明書に基づいてデータ通信先との相互認証または暗号処理データ通信を実行する構成を有することを特徴とする情報処理装置。

【請求項１２】

予め取得した個人識別データであるテンプレートと、ユーザの入力したサンプリング情報との照合により個人認証を実行する情報処理方法において、

前記テンプレートを含むテンプレート情報を暗号化して格納し、第三者機関である個人識別認証局が生成した個人識別証明書から暗号化テンプレートを取得し、

該個人識別証明書に格納されたリンク情報に従って公開鍵証明書を特定し、該特定された公開鍵証明書に基づいてテンプレートの暗号処理鍵を特定し、

テンプレートの暗号化または復号処理を実行することを特徴とする情報処理方法。

【請求項１３】

予め取得した個人識別データであるテンプレートと、ユーザの入力したサンプリング情報との照合により個人認証を実行する情報処理方法において、

第三者機関である個人識別認証局が生成した個人識別証明書から暗号化テンプレートを取得し、テンプレートに基づいて個人認証処理を実行し、

該個人識別証明書に格納されたリンク情報に従って公開鍵証明書を特定し、該特定された公開鍵証明書に基づいてデータ通信先との相互認証または暗号処理データ通信を実行することを特徴とする情報処理方法。

【請求項１４】

予め取得した個人識別データであるテンプレートと、ユーザの入力したサンプリング情報との照合により個人認証処理をコンピュータ・システム上で実行せし

めるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

前記テンプレートを含むテンプレート情報を暗号化して格納し、第三者機関である個人識別認証局が生成した個人識別証明書から暗号化テンプレートを取得するステップと、

該個人識別証明書に格納されたリンク情報に従って公開鍵証明書を特定し、該特定された公開鍵証明書に基づいてテンプレートの暗号処理鍵を特定するステップと、

テンプレートの暗号化または復号処理を実行するステップと、

を有することを特徴とするプログラム提供媒体。

【請求項１５】

予め取得した個人識別データであるテンプレートと、ユーザの入力したサンプリング情報との照合により個人認証処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

第三者機関である個人識別認証局が生成した個人識別証明書から暗号化テンプレートを取得し、テンプレートに基づいて個人認証処理を実行するステップと、

該個人識別証明書に格納されたリンク情報に従って公開鍵証明書を特定し、該特定された公開鍵証明書に基づいてデータ通信先との相互認証または暗号処理データ通信を実行するステップと、

を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は個人識別証明書リンクシステム、情報処理装置、および情報処理方法、並びにプログラム提供媒体に関する。特に、インターネット等の通信ネットワークあるいは媒体を介するデータ通信において、通信相手の個人の識別を実行したり、あるいはＰＣ等、特定の情報処理装置を使用する個人を認証する際に有用な個人識別証明書リンクシステム、情報処理装置、および情報処理方法、並びに

プログラム提供媒体に関する。

【０００２】

【従来の技術】

企業あるいは個人においてデータ処理装置、例えばパーソナルコンピュータ（ＰＣ）等の様々なデータ処理装置が盛んに使用され、このような装置には様々な機密データが格納される場合がある。このような機密情報に対する不正なユーザのアクセスを排除するため、ＰＣに格納された情報の漏洩を防止する技術が開発されており、例えば、パスワード入力、ユーザの生体情報によるユーザ識別処理等が開発されている。

【０００３】

さらに、昨今、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはＤＶＤ、ＣＤ等の流通可能な記憶媒体（メディア）を介して流通している。このような状況の中で、コンテンツの配布あるいはコンテンツ利用料金の回収等、様々な処理において、ユーザ識別処理を確実に迅速に実行し、かつ、識別処理において用いられる個人情報の漏洩の防止が重要な課題となっている。

【０００４】

一般的なユーザ識別方法としては、例えばユーザＩＤ、パスワード等を予め設定し、設定データと入力データとを照合する処理方法がある。しかし、この方法は、登録されているユーザＩＤ，パスワードの漏洩のおそれが常に存在し、一旦漏洩した場合には、同一のユーザＩＤ，パスワードの使用は不可能となる。このような問題点を解決する手法として、生体情報を用いたユーザ識別手法がある。

【０００５】

従来から行われている生体情報を用いた個人識別処理の一例について説明する。代表的例として指紋読み取り照合処理を実行する個人認証装置について図１を用いて説明する。図１に示すＰＣ２０の利用者は、予め、個人の指紋情報を読み取り装置を持つ個人認証装置１０に登録し、このデータをセキュアメモリ１４内に格納する。格納された指紋情報をテンプレート（Template）と呼ぶ。ユーザは

パソコン２０などのデータを利用する際に、指紋読み取り装置として構成された個人認証装置１０により指紋の照合処理を実行させる。

【０００６】

ユーザは、例えばＣＣＤカメラによって構成される個人情報取得部１１において指紋情報の読み取りを実行する。読み取られた指紋情報は、情報変換部１２で特徴抽出処理が実行され、比較部１３にて、セキュアメモリ１４に格納されたテンプレートと、個人情報取得部１１で取得され、特徴抽出されたデータとの比較処理が行われる。

【０００７】

比較部１３における比較処理においては、比較部に予め設定したしきい値により一致、不一致の判定がコントロールされる。比較対照の両データが設定しきい値を越えて一致していればＯＫ、しきい値以下の一致度であればＮＧとなる。なお、指紋情報は指紋画像データそのもので、情報変換部１２で特徴抽出されたデータと、この画像データの比較を行い、しきい値と比較することになる。

【０００８】

比較部１３での判定処理において、入力情報と登録情報が一致すると判定された場合には、通信部１６を経由してパソコン２０に照合成功が伝えられ、ＰＣ２０に対するアクセスが許可される。一致していないと判定された場合には照合失敗が伝えられ、ＰＣ２０に対するアクセスが拒否される。なお、個人認証装置１０は、図１に示すように複数のユーザ（ユーザＩＤ＝ＩＤ１～ＩＤｎ）の指紋情報テンプレートをセキュアメモリに格納し、いずれかの格納テンプレートと一致したことを条件としてＰＣのアクセスを許可する構成とすることで、一台の個人認証装置で複数のユーザに対応することが可能となる。

【０００９】

【発明が解決しようとする課題】

しかしながら、このような個人認証装置では、テンプレートは指紋読み取り照合装置内のメモリに保存される構成であり、以下のような問題点がある。

（ａ）照合結果を利用するには、テンプレートを保持している指紋読み取り照合装置を使用する必要がある。

（ｂ）複数の場所で指紋照合を行う場合、あらかじめ複数の指紋読み取り照合装置に指紋登録を行なう必要がある。

（ｃ）テンプレートが指紋読み取り照合装置内にあるため、テンプレート情報としてのデータを改竄、読み取りされる危険がある。

（ｄ）照合結果をＰＣ等に転送しているため、その結果を攻撃されやすい。

【００１０】

このように、従来の個人認証システムは、機密情報を扱う特定のＰＣ等のデータ処理装置に不可分に構成され、そのＰＣを扱うユーザ専用の認証に重点が置かれており、テンプレートを保存していない機器を使用する場合の認証には全く利用できない。また、テンプレートを格納しているのは指紋読み取り照合装置自体であり、テンプレートの安全性、信頼性といった面で問題がある。

【００１１】

さらに、昨今の暗号化データを使用したネットワークを介するデータ送受信、あるいは媒体を介するデータ配信においては、公開鍵暗号方式による暗号処理、および公開鍵の信頼性を保証する公開鍵証明書が多く使用されている。しかしながら、公開鍵証明書は、公開鍵の保証を行なうものの、公開鍵とその公開鍵の所有者である個人の結び付きを保証することはできないという問題点がある。すなわち、

（ｅ）暗号化データの送信等に使用される公開鍵証明書とその公開鍵の所有者個人との関係を保証する方法がなく、公開鍵の所有者の識別手段が十分ではなかった。

【００１２】

このように、従来の個人認証システムには、様々な解決すべき問題点が存在する。特に、昨今のインターネット等、通信システムの発達したネットワーク社会においては、様々な場所、時間に、多様な通信機器、データ処理機器を用いて機密情報、個人情報を扱う機会が増大している。また、特定のユーザ、例えば会員向けのコンテンツ配信、有料コンテンツの配信システム、サービス等においては、コンテンツ、サービスの配信時にユーザの識別処理を実行することが必要となる。このような状況において、場所、時間、使用機器等の環境に依存しない個人

認証処理システムの実現要求が高まっている。

【００１３】

本発明は、上述の状況に鑑みてなされたものであり、個人認証を様々な環境下において実行でき、さらに個人認証の信頼性を高め、安全なテンプレート情報の格納、利用形態を実現し、さらに公開鍵証明書との関連した使用態様を実現することにより、個人認証の多様な分野での利用を可能とした個人識別証明書リンクシステム、情報処理装置、および情報処理方法、並びにプログラム提供媒体を提供することを目的とする。

【００１４】

特に、本発明は、暗号処理鍵である公開鍵を格納し、認証局が生成する公開鍵証明書と、個人識別データであるテンプレートを格納し、個人識別認証局が生成する個人識別証明書との間で、証明書を関連づけたリンクを形成し、１つの証明書に基づいて他の関連証明書を特定可能とすることにより、効率的な処理を可能とした個人識別証明書リンクシステム、情報処理装置、および情報処理方法、並びにプログラム提供媒体を提供することを目的とする。

【００１５】

【課題を解決するための手段】

本発明の第1の側面は、

暗号処理鍵である公開鍵を格納し、認証局が生成する公開鍵証明書と、個人識別データであるテンプレートを格納し、個人識別認証局が生成する個人識別証明書との間で、２以上の証明書を関連づけたリンクを形成し、１つの証明書に基づいて他の関連証明書を特定可能とした構成を有することを特徴とする個人識別証明書リンクシステムにある。

【００１６】

さらに、本発明の個人識別証明書リンクシステムの一実施態様において、前記証明書のリンクは、個人識別証明書と、該個人識別証明書の格納テンプレートの暗号化に適用した公開鍵の公開鍵証明書とを関連付けたリンクであることを特徴とする。

【００１７】

さらに、本発明の個人識別証明書リンクシステムの一実施態様において、前記証明書のリンクは、データ通信先との接続処理の際に適用する個人識別証明書と公開鍵証明書との組合わせを関連付けたリンクであることを特徴とする。

【００１８】

さらに、本発明の個人識別証明書リンクシステムの一実施態様において、前記公開鍵証明書または前記個人識別証明書は、リンクを持つ異なる証明書の識別子をデータとして格納した構成であることを特徴とする。

【００１９】

さらに、本発明の個人識別証明書リンクシステムの一実施態様において、前記公開鍵証明書または前記個人識別証明書は、リンク識別データとしてのリンク構造体識別子と、リンクを構成する公開鍵証明書識別子と、個人識別証明書識別子とをデータとして格納した構成であることを特徴とする。

【００２０】

さらに、本発明の個人識別証明書リンクシステムの一実施態様において、リンクを構成する公開鍵証明書の識別子と、個人識別証明書との識別子との組データを格納した組情報を、各証明書と別のデータとして構成し管理する構成としたことを特徴とする。

【００２１】

さらに、本発明の個人識別証明書リンクシステムの一実施態様において、リンクを構成する公開鍵証明書の識別子と、個人識別証明書との識別子との組データを格納した組情報を、各証明書と別のデータとして構成し管理し、さらに、前記組情報を一次情報として、前記組情報に関連する二次情報を前記一次情報から特定可能としたリンクを形成したことを特徴とする。

【００２２】

さらに、本発明の個人識別証明書リンクシステムの一実施態様において、前記公開鍵証明書または前記個人識別証明書は、リンクを持つ異なる証明書を格納した構成であることを特徴とする。

【００２３】

さらに、本発明の個人識別証明書リンクシステムの一実施態様において、前記

認証局、前記個人識別認証局は、公開鍵証明書および個人識別証明書の利用当時者以外の第三者機関として構成されていることを特徴とする。

【００２４】

さらに、本発明の第2の側面は、

予め取得した個人識別データであるテンプレートと、ユーザの入力したサンプリング情報との照合により個人認証を実行する情報処理装置において、

前記テンプレートを含むテンプレート情報を暗号化して格納し、第三者機関である個人識別認証局が生成した個人識別証明書から暗号化テンプレートを取得するとともに、該個人識別証明書に格納されたリンク情報に従って公開鍵証明書を特定し、該特定された公開鍵証明書に基づいてテンプレートの暗号処理鍵を特定し、テンプレートの暗号化または復号処理を実行する構成を有することを特徴とする情報処理装置にある。

【００２５】

さらに、本発明の第3の側面は、

予め取得した個人識別データであるテンプレートと、ユーザの入力したサンプリング情報との照合により個人認証を実行する情報処理装置において、

第三者機関である個人識別認証局が生成した個人識別証明書から暗号化テンプレートを取得し、テンプレートに基づいて個人認証処理を実行するとともに、

該個人識別証明書に格納されたリンク情報に従って公開鍵証明書を特定し、該特定された公開鍵証明書に基づいてデータ通信先との相互認証または暗号処理データ通信を実行する構成を有することを特徴とする情報処理装置にある。

【００２６】

さらに、本発明の第4の側面は、

予め取得した個人識別データであるテンプレートと、ユーザの入力したサンプリング情報との照合により個人認証を実行する情報処理方法において、

前記テンプレートを含むテンプレート情報を暗号化して格納し、第三者機関である個人識別認証局が生成した個人識別証明書から暗号化テンプレートを取得し、

該個人識別証明書に格納されたリンク情報に従って公開鍵証明書を特定し、該

特定された公開鍵証明書に基づいてテンプレートの暗号処理鍵を特定し、

テンプレートの暗号化または復号処理を実行することを特徴とする情報処理方法にある。

【００２７】

さらに、本発明の第５の側面は、

予め取得した個人識別データであるテンプレートと、ユーザの入力したサンプリング情報との照合により個人認証を実行する情報処理方法において、

第三者機関である個人識別認証局が生成した個人識別証明書から暗号化テンプレートを取得し、テンプレートに基づいて個人認証処理を実行し、

該個人識別証明書に格納されたリンク情報に従って公開鍵証明書を特定し、該特定された公開鍵証明書に基づいてデータ通信先との相互認証または暗号処理データ通信を実行することを特徴とする情報処理方法にある。

【００２８】

さらに、本発明の第６の側面は、

予め取得した個人識別データであるテンプレートと、ユーザの入力したサンプリング情報との照合により個人認証処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

前記テンプレートを含むテンプレート情報を暗号化して格納し、第三者機関である個人識別認証局が生成した個人識別証明書から暗号化テンプレートを取得するステップと、

該個人識別証明書に格納されたリンク情報に従って公開鍵証明書を特定し、該特定された公開鍵証明書に基づいてテンプレートの暗号処理鍵を特定するステップと、

テンプレートの暗号化または復号処理を実行するステップと、

を有することを特徴とするプログラム提供媒体にある。

【００２９】

さらに、本発明の第７の側面は、

予め取得した個人識別データであるテンプレートと、ユーザの入力したサンプ

リング情報との照合により個人認証処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

第三者機関である個人識別認証局が生成した個人識別証明書から暗号化テンプレートを取得し、テンプレートに基づいて個人認証処理を実行するステップと、

該個人識別証明書に格納されたリンク情報に従って公開鍵証明書を特定し、該特定された公開鍵証明書に基づいてデータ通信先との相互認証または暗号処理データ通信を実行するステップと、

を有することを特徴とするプログラム提供媒体にある。

【００３０】

本発明の第６、７の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯ、ＤＶＤなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００３１】

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００３２】

【発明の実施の形態】

以下、図面を参照しながら、本発明の実施の形態について詳細に説明する。

【００３３】

【実施例】

以下、本発明の構成について、下記の項目順に説明する。

１．本発明の概念と証明書概要

２．テンプレートの暗号化

３．テンプレート、個人識別証明書（ＩＤＣ）の登録、変更処理

４．個人識別証明書（ＩＤＣ）の基本的利用形態

５．個人識別証明書（ＩＤＣ）を使用した認証処理態様

６．個人識別証明書に基づくユーザ認証によるコンテンツの利用権制御処理

７．個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）とのリンク

８．個人識別証明書（ＩＤＣ）による認証と公開鍵証明書（ＰＫＣ）に基づくコンテンツ利用処理

９．ワンタイム公開鍵証明書（ワンタイムＰＫＣ）

１０．照合証明書

１１．個人識別証明書（ＩＤＣ）のダウンロードおよびコンテンツ利用処理

１２．個人識別証明書（ＩＤＣ）の有効期限設定

【００３４】

［１．本発明の概念と証明書概要］

（１．１．本発明のシステムの基本概念）

まず、本発明の個人認証システムの基本概念について説明する。本発明の個人認証は個人識別証明書（ＩＤＣ：Identification Certificate）を使用することによって実現される。個人識別証明書（ＩＤＣ）は、信頼できる第三者機関である個人識別認証局（ＩＤＡ：Identification Authority）が証明対象となる個人各々について、個人の確認を行なった上で発行する証明書である。

【００３５】

個人識別証明書（ＩＤＣ）には、各個人を識別するための情報（テンプレート情報）が格納される。個人識別情報としては、例えば指紋情報、網膜情報、虹彩情報、声紋情報、筆跡情報が使用可能であり、さらに生体情報以外の個人識別情報、例えば印鑑、パスポート、免許書、カード等の識別データ、あるいは、上記各情報の組合わせ、または、上記各情報とパスワードとの組み合わせ等、基本的に本人のみが持ち得る情報が使用され、これらの個人識別情報が原則として暗号

化されて、テンプレート情報として格納される。

【００３６】

個人識別認証局（ＩＤＡ）により発行された個人識別証明書（ＩＤＣ）は、その登録者自身であるユーザ、または登録者であるユーザに対してコンテンツ配信を行なうサービスプロバイダ（ＳＰ）、あるいは利用者確認を必要とする様々な機関（例えば決済金融機関等）、あるいはユーザデバイスからの要求に応じて、個人識別認証局（ＩＤＡ）から提供され、個人識別のために利用される。具体的な利用形態については、後段で詳細に説明する。

【００３７】

さらに、本発明の個人識別証明書（ＩＤＣ）は、公開鍵証明書（ＰＫＣ：Public Key Certificate）との組み合わせにおいて有効な利用形態が実現される。すなわち、コンテンツの暗号化配信を行なうサービスプロバイダ（ＳＰ）が個人の識別処理を行う際に個人識別証明書（ＩＤＣ）を利用し、識別された個人にのみ復号可能な暗号化データの配信を公開鍵証明書を用いた公開鍵暗号方式により行なうことを可能とする。

【００３８】

図２に本発明の個人認証システムを利用し、かつ公開鍵証明書を用いた暗号化データ通信の概略を説明する図を示す。上述の個人識別証明書（ＩＤＣ）を発行する個人識別認証局（ＩＤＡ）２０１、また公開鍵証明書（ＰＫＣ）を発行する認証局（ＣＡ：Certificate Authority）２０２においてそれぞれの証明書が所定の手続きにより発行される。

【００３９】

暗号化データ通信は、例えばコンテンツ配信を行なうサービスプロバイダ（ＳＰ）２０３と、ユーザデバイスＡ２０５の間において実行される。この際、サービスプロバイダ（ＳＰ）２０３は、ユーザデバイスＡの使用者がユーザＡであることを確認し、ユーザＡにおいて復号可能な暗号化データを生成してコンテンツの暗号化配信を行なう。

【００４０】

ユーザＡは、個人情報を個人識別認証局（ＩＤＡ）２０１に登録することによ

り、個人識別認証局（ＩＤＡ）２０１から個人識別証明書（ＩＤＣ）の発行を受けており、個人識別証明書（ＩＤＣ）により、サービスプロバイダ（ＳＰ）２０３はユーザＡであることの確認を行なう。この場合、サービスプロバイダ（ＳＰ）２０３が個人識別証明書（ＩＤＣ）による個人認証を実行するエンティテイとなる。個人識別証明書による確認処理態様には各種あるが、これらについては後段で詳細に説明する。

【００４１】

また、ユーザＡは、ユーザ自身の公開鍵を認証局２０２に提出し、認証局の電子署名入りの公開鍵証明書の発行を受ける。サービスプロバイダ（ＳＰ）２０３が個人識別証明書（ＩＤＣ）に基づいてユーザＡであることの確認を行なった後、例えば、サービスプロバイダ（ＳＰ）２０３は、ユーザＡの公開鍵証明書から公開鍵を取り出して、取り出した公開鍵によってコンテンツを暗号化して、コンテンツをユーザＡに対して配信する。暗号化コンテンツの配信を受けたユーザデバイスＡ２０５のユーザＡは、公開鍵とペアになった秘密鍵によって配信された暗号化データを復号して利用する。

【００４２】

また、決済機関としてのサービスプロバイダ（ＳＰ）２０４と、ユーザデバイスＢ２０６との間においても、上述と同様にサービスプロバイダ（ＳＰ）２０４によるユーザＢの個人識別証明書に基づくユーザＢの確認、さらにユーザＢの公開鍵証明書を用いた暗号化データ（例えばコンテンツデータ、決済データ等）の送受信が行われる。この場合、ユーザデバイスが個人識別証明書（ＩＤＣ）による個人認証を実行するエンティテイとなる。

【００４３】

さらに、ユーザデバイスＡ２０５と、ユーザデバイスＢ２０６との間のデータ通信においても、ユーザＡ，Ｂの個人識別証明書に基づくユーザＡ，Ｂの確認、ユーザＡまたはユーザＢの公開鍵証明書を用いた暗号化データの送受信が行われる。

【００４４】

このように、様々な形態でのデータ送受信において、個人識別証明書および公

開鍵証明書が利用可能である。個人識別証明書単独の利用形態も可能であり、機密情報を格納したＰＣ等に対するアクセス時に個人識別証明書による照合処理によりユーザ確認を行なうこともちろん可能である。個人識別証明書による個人認証を実行するエンテイテイは、サービスプロバイダ（ＳＰ）、ユーザデバイス、さらに個人識別認証局（ＩＤＡ）等、様々なエンティテイである。

【００４５】

また、図２に示すように、本発明のシステムの一実施例として、個人識別認証局（ＩＤＡ）２０１の発行する個人識別証明書（ＩＤＣ）と、認証局２０２の発行する公開鍵証明書（ＰＫＣ）をリンクさせた構成がある。リンク構成には、個人識別証明書の中に公開鍵証明書（ＰＫＣ）を含ませる構成としたり、リンク情報体としての組情報を生成する構成等がある。これらのリンク構成については、後段で詳細に説明する。

【００４６】

上述の説明における公開鍵暗号方式は、発信者と受信者の鍵を異なるものとして、一方の鍵を不特定のユーザが使用可能な公開鍵として、他方を秘密に保つ秘密鍵とするものである。公開鍵暗号方式では、暗号化、復号化に共通の鍵を用いるいわゆる共通鍵暗号化方式と異なり、秘密に保つ必要のある秘密鍵は、特定の１人が持てばよいため鍵の管理において有利である。公開鍵暗号方式の代表的なものにはＲＳＡ（Rivest-Shamir-Adleman）暗号がある。これは非常に大きな２つの素数（例えば１５０桁）の積を用いるものであり、大きな２つの素数（例えば１５０桁）の積の素因数分解処理の困難性を利用している。

【００４７】

公開鍵暗号方式では、不特定多数に公開鍵を使用可能とする構成であり、配布する公開鍵が正当なものであるか否かを証明する証明書、いわゆる公開鍵証明書を使用する方法が多く用いられている。例えば、利用者Ａが公開鍵、秘密鍵のペアを生成して、生成した公開鍵を認証局に対して送付して公開鍵証明書を認証局から入手する。利用者Ａは公開鍵証明書を一般に公開する。不特定のユーザは公開鍵証明書から所定の手続きを経て公開鍵を入手して文書等を暗号化して利用者Ａに送付する。利用者Ａは秘密鍵を用いて暗号化文書等を復号する等のシステム

である。また、利用者Ａは、秘密鍵を用いて文書等に署名を付け、不特定のユーザが公開鍵証明書から所定の手続きを経て公開鍵を入手して、その署名の検証を行なうことができる。以下、本発明の個人認証システムの具体的説明に先立ち、本発明のシステムにおいて用いられる公開鍵証明書（ＰＫＣ）および個人識別証明書（ＩＤＣ）のデータ構成について説明する。

【００４８】

（１．２．公開鍵証明書）

公開鍵証明書について図３，４を用いて説明する。公開鍵証明書は、公開鍵暗号方式における認証局（ＣＡ：Certificate AuthorityまたはＩＡ：Issuer Authority）が発行する証明書であり、ユーザが自己のＩＤ、公開鍵等を認証局に提出することにより、認証局側が認証局のＩＤや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

【００４９】

公開鍵証明書のフォーマット例を示す。これは、公開鍵証明書フォーマットＸ．５０９　Ｖ３に準拠した例である。

【００５０】

バージョン（version）は、証明書フォーマットのバージョンを示す。

シリアルナンバ（Serial Number）は、公開鍵証明書発行局（ＩＡ）によって設定される公開鍵証明書のシリアルナンバである。

署名アルゴリズム識別子、アルゴリズムパラメータ（Signature algorithm Identifier algorithm parameter）は、公開鍵証明書の署名アルゴリズムとそのパラメータを記録するフィールドである。なお、署名アルゴリズムとしては、楕円曲線暗号およびＲＳＡがあり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、ＲＳＡが適用されている場合には鍵長が記録される。

発行者（issuer）は、公開鍵証明書の発行者、すなわち公開鍵証明書発行局（ＩＡ）の名称が識別可能な形式（Distinguished Name）で記録されるフィールドである。

有効期限(validity)は、証明書の有効期限である開始日時、終了日時が記録される。

サブジェクト(subject)は、ユーザである認証対象者の名前が記録される。具体的には例えばユーザ機器のＩＤや、サービス提供主体のＩＤ等である。

サブジェクト公開鍵情報（subject Public Key Info algorithm subject Public key）は、ユーザの公開鍵情報としての鍵アルゴリズム、鍵情報そのものを格納するフィールドである。

【００５１】

ここまでが、公開鍵証明書フォーマットＸ．５０９　Ｖ１に含まれるフィールドであり、以下は、公開鍵証明書フォーマットＸ．５０９　Ｖ３において追加されるフィールドである。

【００５２】

証明局鍵識別子（authority Key Identifier－key Identifier、authority Cert Issuer、authority Cert Serial Number）は、公開鍵証明書発行局（ＩＡ）の鍵を識別する情報であり、鍵識別番号（８進数）、公開鍵証明書発行局（ＩＡ）の名称、認証番号を格納する。

サブジェクト鍵識別子（subject key Identifier）は、複数の鍵を公開鍵証明書において証明する場合に各鍵を識別するための識別子を格納する。

鍵使用目的（key usage）は、鍵の使用目的を指定するフィールドであり、（０）ディジタル署名用、（１）否認防止用、（２）鍵の暗号化用、（３）メッセージの暗号化用、（４）共通鍵配送用、（５）認証の署名確認用、（６）失効リストの署名確認用の各使用目的が設定される。

秘密鍵有効期限(private Key Usage Period)は、ユーザの有する秘密鍵の有効期限を記録する。

認証局ポリシー（certificate Policies）は、認証局、ここでは、公開鍵証明書発行局（ＩＡ）および登録局（ＲＡ）の証明書発行ポリシーを記録する。例えばＩＳＯ／ＩＥＣ９３８４－１に準拠したポリシーＩＤ、認証基準である。

ポリシー・マッピング（policy Mapping）は、ＣＡ（公開鍵証明書発行局（ＩＡ））を認証する場合にのみ記録するフィールドであり、証明書発行を行なう公開鍵証明書発行局（ＩＡ）のポリシーと、被認証ポリシーのマッピングを規定する。

サポート・アルゴリズム（supported Algorithms）は、ディレクトリ（X．５００）のアトリビュートを定義する。これは、コミュニケーションの相手がディレクトリ情報を利用する場合に、事前にそのアトリビュートを知らせるのに用いる。

サブジェクト別名（subject Alt Name）は、ユーザの別名を記録するフィールドである。

発行者別名（issuer Alt Name）は、証明書発行者の別名を記録するフィールドである。

サブジェクト・ディレクトリ・アトリビュート（subject Directory Attribute）は、ユーザの任意の属性を記録するフィールドである。

基本制約（basic Constraint）は、証明対象の公開鍵が認証局（公開鍵証明書発行局（ＩＡ））の署名用か、ユーザのものかを区別するためのフィールドである。

許容サブツリー制約名（name Constraints permitted Subtrees）は、被認証者が認証局（公開鍵証明書発行局（ＩＡ））である場合にのみ使用される証明書の有効領域を示すフィールドである。

制約ポリシー（policy Constraints）は、認証パスの残りに対する明確な認証ポリシーＩＤ、禁止ポリシーマップを要求する制限を記述する。

ＣＲＬ参照ポイント（Certificate Revocation List Distribution Points）は、ユーザが証明書を利用する際に、証明書が失効していないか、どうかを確認するための失効リスト（図９参照）の参照ポイントを記述するフィールドである。

署名は、公開鍵証明書発行者（公開鍵証明書発行局（ＩＡ））の署名フィールドである。電子署名は、証明書全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。

【００５３】

認証局は、図３，４に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リスト

の作成、管理、配布（これをリボケーション：Revocationと呼ぶ）を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

【００５４】

一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。

【００５５】

（１．３．個人識別証明書）

本発明の個人認証システムにおいて用いられる個人識別証明書（ＩＤＣ）には、個人識別のための情報（以下、このＩＤＣに含まれる個人識別情報をテンプレート情報と呼ぶ）が含まれる。テンプレート情報は、個人の生体（バイオメトリクス）情報、例えば指紋情報、網膜情報、虹彩情報、声紋情報、筆跡情報が使用可能であり、さらに生体情報以外の個人識別情報、例えば印鑑、パスポート、免許書、カード等の識別データ、あるいは、上記各情報の組合わせ、または、上記各情報とパスワードとの組み合わせ等、基本的に本人のみが持ち得る情報が使用可能である。このようなテンプレート情報は、不正な第三者に漏洩することがないように暗号化してＩＤＣに格納することが望ましい。ただし、個人識別証明書の流通範囲が極めて限定され、秘密の漏洩防止が確実に実現されることが保証される環境であれば、テンプレートの暗号化は必ずしも必要ではない。

【００５６】

また、個人識別証明書（ＩＤＣ）には、個人識別認証局（ＩＤＡ）のデジタル署名がなされ、個人識別証明書の改竄が防止される構成となっている。

【００５７】

個人識別証明書のフォーマット例を図５に示す。図５の個人識別証明書は、必須項目フィールドと、拡張項目フィールド、そして、署名フィールドに大別される。各項目について説明する。

【００５８】

まず、必須項目の各フィールドについて説明する。

バージョン（version）は、証明書フォーマットのバージョンを示す。

認証番号（Serial Number）は、個人識別認証局（ＩＤＡ）によって設定される各個人識別証明書（ＩＤＣ）のシリアルナンバである。

署名方式（Signature algorithm Identifier algorithm parameter）は、個人識別証明書の署名アルゴリズムとそのパラメータを記録するフィールドである。なお、署名アルゴリズムとしては、楕円曲線暗号およびＲＳＡがあり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、ＲＳＡが適用されている場合には鍵長が記録される。

発行者（issuer）は、個人識別証明書の発行者、すなわち個人識別認証局（ＩＤＡ）の名称が識別可能な形式（Distinguished Name）で記録されるフィールドである。

有効期限(validity)は、証明書の有効期限である開始日時、終了日時が記録される。

サブジェクト(subject)は、ユーザである認証対象者の名前が記録される。具体的には例えばユーザのＩＤや、氏名等である。

テンプレート情報（Subject Template Info）は、ユーザの個人識別情報として、例えば前述した指紋等の生体情報のデータを暗号化して格納するフィールドであり、テンプレートの暗号化方式、暗号化するために使用した公開鍵証明書の固有識別子（ＩＤ）または認証番号、暗号化アルゴリズム、パラメータ、テンプレートの有効期限としての開始日時、終了日時、テンプレートの種別、テンプレート（暗号化）の各情報が格納される。

ここまでが、必須項目フィールドとして設定される。

【００５９】

以下は、個人識別証明書（ＩＤＣ）における拡張フィールドである。

被認証者の公開鍵証明書情報（Subject PKC info）には、被認証者の公開鍵証明書情報としての、被認証者の公開鍵証明書の認証番号、被認証者の公開鍵証明書の被認証者固有ＩＤが格納される。

個人識別認証局の固有ＩＤ（Issuer Unique ID）は、個人識別認証局（ＩＤＡ

）の固有ＩＤを格納する。

被認証者の固有ＩＤ（Subject Unique ID）は、被認証者の固有ＩＤを格納する。

公開鍵証明書（Public Key Certificate）は、前述した公開鍵証明書を格納する。

個人識別認証局の別名（Issuer Alt Name）は、個人識別認証局の別名を格納する。

個人情報（Subject Directory Attribute）は、本人確認のための情報として、ユーザの任意の属性、例えば、年齢、性別、住所、電話番号等の個人情報が必要に応じて暗号化されて格納される。

有効回数（Valid Count）は、個人識別証明書による個人認証処理の制限回数を記録するフィールドである。１度発行した証明書の利用を制限回数内にとどめるための設定数を記録する。

組情報へのリンク情報(Control Table link Info)は、個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）とのリンク情報としての組情報を格納する。例えば、個人識別証明書による個人認証処理を条件として実行されるデータ通信、データ処理において使用される公開鍵証明書とのリンク情報を格納する。リンク情報、組情報については後段で詳細に説明する。

以上が、個人識別証明書（ＩＤＣ）における拡張フィールドの内容である。

【００６０】

電子署名は、証明書を構成する各フィールドの全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して個人識別認証局（ＩＤＡ）の秘密鍵を用いて生成したデータである。

【００６１】

なお、個人識別証明書（ＩＤＣ）における拡張フィールドには、さらに他の情報を格納してもよい。例えばテンプレート情報を公開鍵ではなく共通の秘密鍵で暗号化し、その暗号化に用いた共通鍵をユーザデバイス、サービスプロバイダ、または個人識別認証局（ＩＤＡ）の公開鍵で暗号化して格納してもよい。この場合の処理形態については後述する。

【００６２】

［２．テンプレートの暗号化］

上述の個人識別証明書（ＩＤＣ）には、個人識別のための情報（テンプレート情報）が含まれる。テンプレート情報は、前述したように、個人の生体（バイオメトリクス）情報、例えば指紋情報、網膜情報、虹彩情報、声紋情報、筆跡情報が使用可能であり、さらに生体情報以外の個人識別情報、例えば印鑑、パスポート、免許書、カード等の識別データ、あるいは、上記各情報の組合わせ、または、上記各情報とパスワードとの組み合わせ等、基本的に本人のみが持ち得る情報であり個人の識別の基礎となる情報である。

【００６３】

テンプレートは、前述したように特定の機密の守られる範囲内での証明書使用に限定される場合以外においては、第三者に対する漏洩を防止するため、暗号化して格納することが望ましい。ここでは、テンプレートの格納態様、暗号化態様について説明する。

【００６４】

テンプレートの格納および暗号化態様としては、以下の態様がある。

１）テンプレートを暗号化しないで格納する。

２）テンプレートをユーザ（個人識別証明書において識別されるユーザ）の公開鍵で暗号化する。

３）テンプレートを共通鍵Ｋｔで暗号化し共通鍵Ｋｔをユーザの公開鍵で暗号化する。

４）テンプレートをサービスプロバイダ（ＳＰ）（個人識別証明書を利用してサービス提供ユーザの識別を実行するＳＰ）の公開鍵で暗号化する。

５）テンプレートを共通鍵Ｋｔで暗号化し共通鍵Ｋｔをサービスプロバイダ（ＳＰ）の公開鍵で暗号化する。

６）テンプレートを個人識別認証局（ＩＤＡ）の公開鍵で暗号化する。

７）テンプレートを共通鍵Ｋｔで暗号化し共通鍵Ｋｔを個人識別認証局（ＩＤＡ）の公開鍵で暗号化する。

【００６５】

上記７種類の態様があるが、これらの処理について図６、図７、図８を用いて説明する。図６（ａ）は、テンプレートを暗号化しない場合の処理であり、個人識別装置から取得した例えば指紋等の生体情報をテンプレート、具体的には指紋データをコード化したデータをそのままテンプレート情報として、個人識別証明書（ＩＤＣ）に格納する。

【００６６】

図６（ｂ）は、公開鍵のみを使用した暗号化、復号処理を示す図であり、（ｂ－１）の暗号化処理においては、個人識別装置から取得したユーザの識別情報であるテンプレートを、そのユーザまたはユーザデバイスの公開鍵、サービスプロバイダ（ＳＰ）（個人識別証明書を利用してサービス提供ユーザの識別を実行するＳＰ）の公開鍵、または、個人識別認証局（ＩＤＡ）の公開鍵のいずれかを用いて暗号化する。暗号化方式は例えば楕円曲線暗号（Elliptic Curve Cryptography（ＥＣＣ）、ＲＳＡ暗号（（Rivest、Shamir、Adleman）が適用される。暗号化されたテンプレートは、そのテンプレートの暗号化処理に適用した暗号方式（アルゴリズム）と、公開鍵の識別子（固有ＩＤ）とともに個人識別証明書（ＩＤＣ）に格納される。

【００６７】

なお、ここで使用される公開鍵は、公開鍵固有ＩＤによって識別可能な公開鍵である。公開鍵固有ＩＤは公開鍵証明書を特定可能な情報であり、例えば公開鍵証明書に格納されたユーザＩＤ、ユーザ名等が使用可能である。使用する公開鍵は、ユーザの公開鍵、サービスプロバイダ（ＳＰ）（個人識別証明書を利用してサービス提供ユーザの識別を実行するＳＰ）の公開鍵、または、個人識別認証局（ＩＤＡ）の公開鍵のいずれかであり、個人識別証明書（ＩＤＣ）の使用形態によって選択される。

【００６８】

図７にテンプレートの暗号化に使用する公開鍵の使用形態の場合分けについて説明する図を示す。例えば、ユーザまたはユーザデバイスの公開鍵をテンプレート暗号化に用いる個人識別証明書（ＩＤＣ）の使用例には、ユーザデバイス（例えばＰＣ）の使用許可を付与した特定ユーザの識別を行なうために使用する個人

識別証明書（ＩＤＣ）がある。ＰＣ使用の際に、個人識別証明書（ＩＤＣ）の格納テンプレートをユーザ秘密鍵で復号し、復号によって得られたテンプレートと入力テンプレートの比較により、各ユーザの個人識別を行なう場合等である。

【００６９】

サービスプロバイダの公開鍵をテンプレート暗号化に用いる個人識別証明書（ＩＤＣ）の使用例としては、サービスプロバイダにおいて特定ユーザ、例えば、サービスを提供するユーザを識別するための個人識別証明書（ＩＤＣ）がある。サービスプロバイダは、サービスプロバイダが保有、あるいはユーザまたは個人識別認証局（ＩＤＡ）から送付される各ユーザの個人識別証明書（ＩＤＣ）から暗号化テンプレート情報を取り出してサービスプロバイダの秘密鍵を用いて復号し、認証処理の対象となる個人の提出したサンプリング情報（指紋データ等）と復号したテンプレートとの照合処理を実行する。

【００７０】

個人識別認証局の公開鍵をテンプレート暗号化に用いる個人識別証明書（ＩＤＣ）の使用例としては、例えば、端末間でのデータ送受信を実行するデータ送受信者において、個人識別認証局（ＩＤＡ）発行の個人識別証明書（ＩＤＣ）を用いて個人識別処理を行なう場合がある。このように、個人識別証明書（ＩＤＣ）の使用形態に応じて、ＩＤＣ内に格納するテンプレート情報の暗号化形態が異なってくる。

【００７１】

図６、（ｂ－２）は、公開鍵暗号方式で暗号化されたテンプレートの復号処理を示す図であり、個人識別証明書（ＩＤＣ）から、暗号化テンプレートを取り出して、さらに、暗号方式、公開鍵固有ＩＤを取り出す。さらに、公開鍵固有ＩＤから特定される公開鍵に対応する秘密鍵を取り出して、取り出した秘密鍵により、暗号化テンプレートの復号処理を実行して、テンプレートを取り出す。個人名認証を実行するユーザデバイスあるいはサービスプロバイダ等の個人認証実行エンティテイは、これらのデータ復号、暗号処理を実行可能な暗号処理部を有する。

【００７２】

図８は、共通鍵と公開鍵とを使用したテンプレート暗号化処理、復号処理を説明する図である。（ｃ－１）は、暗号化処理のプロセスを説明したものであり、まず、暗号化テンプレート情報を生成しようとする例えば個人識別認証局（ＩＤＡ）において、乱数から共通鍵を生成し、個人識別装置から入力されたテンプレートに対して、共通鍵で暗号化を実行する。さらに、そのユーザまたはユーザデバイスの公開鍵、サービスプロバイダ（ＳＰ）の公開鍵、または、個人識別認証局（ＩＤＡ）の公開鍵のいずれか適用する公開鍵を共通鍵を用いて暗号化する。これらの公開鍵の選択は、前述した図７の使用態様に応じて行なうものである。

【００７３】

このようにして生成された暗号化テンプレートおよび暗号化共通鍵を、テンプレート暗号化、共通鍵暗号化に適用した暗号方式（アルゴリズム）と、公開鍵の識別子（固有ＩＤ）とともに個人識別証明書（ＩＤＣ）に格納する。

【００７４】

（ｃ－２）は、共通鍵と秘密鍵とを使用した復号処理を示す図であり、個人識別証明書（ＩＤＣ）の暗号化テンプレート情報から、暗号化テンプレートを取り出して、さらに、暗号化された共通鍵、暗号方式、公開鍵固有ＩＤを取り出す。さらに、公開鍵固有ＩＤから特定される公開鍵により特定される秘密鍵を用いて暗号化共通鍵の復号を実行し、復号して得られる共通鍵に基づいて、暗号化テンプレートの復号処理を実行して、テンプレートを取り出す。

【００７５】

［３．テンプレート、個人識別証明書（ＩＤＣ）の登録、変更処理］

次に上述したデータ内容を持つ個人識別証明書（ＩＤＣ）の登録、削除、変更、追加、停止、停止解除処理について説明する。なお、停止は、ＩＤＣの有効性を一旦停止する処理であり、停止解除処理は、一旦、有効性が停止されたＩＤＣを再度有効にする処理である。

【００７６】

（３．１．テンプレート登録）

個人識別証明書（ＩＤＣ）を有効に登録するには、まず、個人識別証明書（ＩＤＣ）の証明対象となる個人がサンプリング情報を提供してテンプレートを登録

することが必要となる。テンプレートは、前述したように、個人の生体（バイオメトリクス）情報、例えば指紋情報、網膜情報、虹彩情報、声紋情報、筆跡情報、生体情報以外の個人識別情報、例えば印鑑、パスポート、免許書、カード等の識別データ、あるいは、上記各情報の組合わせ、または、上記各情報とパスワードとの組み合わせ等、基本的に本人のみが持ち得る情報を含む情報である。

【００７７】

テンプレート登録、ＩＤＣ生成処理の流れを図９に示す。テンプレートの登録処理は、上記各種の態様の個人情報を採取可能な装置を用いて採取された情報（サンプリング情報）に基づいて行なう。例えば指紋情報をテンプレートとして用いる場合は指紋読み取り装置、声紋情報を使用する場合は、声紋情報の取得装置を用いて採取する（Ｓ１１）。取得データは、オンラインまたはオフラインにより個人識別認証局（ＩＤＡ）に送られる（Ｓ１２）。また、ユーザは個人情報（ＰＩＮ）を本人確認のために個人識別認証局（ＩＤＡ）に送る（Ｓ１３）。

【００７８】

これらのデータがオンラインで送られる場合は、ユーザのデバイスと個人識別認証局（ＩＤＡ）間での相互認証処理が実行され、転送データには電子署名が付加され、データ受信側では署名検証が実行される。個人識別認証局（ＩＤＡ）はデータの改竄チェックを実行し、本人確認を実行し、データ正当性の検証を行なう（Ｓ１４）。正当性が確認されない場合はエラー（Ｓ１７）として登録処理は実行されない。

【００７９】

個人識別認証局（ＩＤＡ）は、テンプレートの登録に際して、本人確認可能な個人証明データにより本人確認処理を実行する。また、必要に応じて住所、連絡先等の個人情報を取得する。個人識別認証局（ＩＤＡ）は、本人確認および必要データの確認の後、テンプレートに個人識別子を割り当て、データベースに格納（Ｓ１５）し、テンプレートを個人識別認証局（ＩＤＡ）の公開鍵で暗号化して、暗号化テンプレートを格納した個人識別証明書（ＩＤＣ）を生成する（Ｓ１６）。なお、ＩＤＣにおけるテンプレートの暗号化鍵は、ＩＤＣの使用場所、すなわち個人認証実行エンティテイに応じて異なって使用される場合があり、例えば

サービスプロバイダ、またはユーザデバイス等の公開鍵を用いて行われることもある。

【００８０】

（３．２．テンプレート削除）

個人識別認証局（ＩＤＡ）に登録したテンプレートは、テンプレート削除処理により、削除可能である。削除処理は、例えば、ユーザからの削除要求により実行される。テンプレート削除処理の流れを図１０に示す。ユーザは、削除要求（Ｓ２１）にともない、ユーザ身元の確認可能な個人証明データを個人識別認証局（ＩＤＡ）に提出する（Ｓ２２）。ユーザは、さらに個人情報（ＰＩＮ）を本人確認のために個人識別認証局（ＩＤＡ）に送る（Ｓ２３）。

【００８１】

これらのデータがオンラインで送られる場合は、ユーザのデバイスと個人識別認証局（ＩＤＡ）間での相互認証処理が実行され、転送データには電子署名が付加され、データ受信側では署名検証が実行される。個人識別認証局（ＩＤＡ）はデータの改竄チェックを実行し、本人確認を実行し、データ正当性の検証を行なう（Ｓ２４）。正当性が確認されない場合はエラー（Ｓ２７）として削除処理は実行されない。

【００８２】

個人識別認証局（ＩＤＡ）は、ユーザ身元の確認を個人証明データにより行い、本人からの要求であることを確認（Ｓ２４）して、削除要求対象のテンプレート、個人識別データ、その他、付加情報の削除を実行する（Ｓ２５）。さらに、テンプレートの格納された個人識別証明書（ＩＤＣ）の削除を行ない、削除されたＩＤＣを失効リストに登録する（Ｓ２６）。具体的には、失効リストに対して対応するＩＤＣ識別子を登録する。

【００８３】

（３．３．テンプレート変更）

個人識別認証局（ＩＤＡ）に登録したテンプレートは、テンプレート変更処理により、変更可能である。テンプレート変更処理の流れを図１１に示す。ユーザは、個人識別認証局（ＩＤＡ）に対してテンプレート変更要求を提出（Ｓ３１）

し、新たなテンプレート生成用のサンプリング情報等を採取し（Ｓ３２）、さらに、身元確認のための個人証明データ、付加情報（ＰＩＮ）を必要に応じて個人識別認証局（ＩＤＡ）に送付する（Ｓ３３，Ｓ３４）。個人識別認証局（ＩＤＡ）は、個人証明データに基づいて個人確認を実行（Ｓ３５）し、変更前のテンプレートに基づく個人識別証明書（ＩＤＣ）を削除（Ｓ３６）し、失効リストに登録（Ｓ３７）する。さらに、新たなテンプレートに識別番号を付与してデータベースに格納（Ｓ３８）し、テンプレートを個人識別認証局（ＩＤＡ）の公開鍵で暗号化して、暗号化テンプレートを格納した個人識別証明書（ＩＤＣ）を生成（Ｓ３９）する。なお、ユーザデバイスと個人識別認証局（ＩＤＡ）との間のオンラインでのデータ通信においては、前述の処理と同様、相互認証処理、通信データの署名付加、検証処理を実行する。

【００８４】

（３．４．テンプレート追加）

ユーザは、個人識別認証局（ＩＤＡ）に登録したテンプレートに、さらに別の個人識別データを追加テンプレートとして追加することができる。テンプレート追加処理の流れを図１２に示す。ユーザは、テンプレート追加要求を個人識別認証局（ＩＤＡ）に実行（Ｓ４１）し、新たなテンプレートを採取装置により採取（Ｓ４２）し、個人識別認証局（ＩＤＡ）に対して個人証明データとともに送付（Ｓ４３，Ｓ４４）する。個人識別認証局（ＩＤＡ）は、受領した個人証明データの検証（Ｓ４５）により、本人確認を実行して、追加テンプレートに対して個人識別子（番号）を割り当ててデータベースに格納（Ｓ４６）し、追加テンプレートを個人識別認証局（ＩＤＡ）の公開鍵で暗号化して、暗号化テンプレートを格納した個人識別証明書（ＩＤＣ）を生成（Ｓ４７）する。なお、ユーザデバイスと個人識別認証局（ＩＤＡ）との間のオンラインでのデータ通信においては、前述の処理と同様、相互認証処理、通信データの署名付加、検証処理を実行する。

【００８５】

（３．５．テンプレート停止）

個人識別認証局（ＩＤＡ）に登録したテンプレートを一次的に使用を停止する

処理がユーザからの停止要求により実行できる。テンプレート停止処理の流れを図１３に示す。ユーザは、テンプレート停止要求を個人識別認証局（ＩＤＡ）に実行（Ｓ５１）し、ユーザは、個人証明データ、付加情報を個人識別認証局（ＩＤＡ）に提出する（Ｓ５２，Ｓ５３）と、個人識別認証局（ＩＤＡ）は、個人証明データにより本人確認を行ない（Ｓ５４）、要求のあったユーザのテンプレート、個人証明データ、付加情報の有効性を停止（Ｓ５５）する。この停止処理の際に、個人識別認証局（ＩＤＡ）は、ユーザの個人識別証明書（ＩＤＣ）の失効処理、失効リスト登録（Ｓ５６）を行なう。具体的には、失効リストに対して対応するＩＤＣ識別子を登録する。なお、ユーザデバイスと個人識別認証局（ＩＤＡ）との間のオンラインでのデータ通信においては、前述の処理と同様、相互認証処理、通信データの署名付加、検証処理を実行する。

【００８６】

（３．６．テンプレート停止解除）

停止処理により、有効性の停止されたテンプレートは、ユーザからの停止解除要求により、有効性を回復することができる。テンプレート停止解除処理の流れを図１４に示す。ユーザは、テンプレート停止解除要求を個人識別認証局（ＩＤＡ）に実行（Ｓ６１）し、ユーザは、個人証明データ、必要な付加情報を個人識別認証局（ＩＤＡ）に提出する（Ｓ６２，Ｓ６３）。個人識別認証局（ＩＤＡ）は個人証明データによる本人確認（Ｓ６４）の後、要求のあったユーザのテンプレート、個人証明データ、付加情報の有効性の停止解除を行なう（Ｓ６５）。さらに、個人識別認証局（ＩＤＡ）は、ユーザの個人識別証明書（ＩＤＣ）が登録された失効リストの更新を行なう（Ｓ６６）。具体的には、失効リストから対応するＩＤＣ識別子を削除する。なお、ユーザデバイスと個人識別認証局（ＩＤＡ）との間のオンラインでのデータ通信においては、前述の処理と同様、相互認証処理、通信データの署名付加、検証処理を実行する。

【００８７】

（３．７．個人識別証明書（ＩＤＣ）配布）

次に、ユーザから提供され、登録されたテンプレートに基づいて生成される個人識別証明書（ＩＤＣ）配布処理について説明する。

【００８８】

図１５にサービスプロバイダ（ＳＰ）に対する個人識別証明書（ＩＤＣ）配布処理の流れを示す。まず、個人識別証明書（ＩＤＣ）を利用しようとするサービスプロバイダは、個人識別認証局（ＩＤＡ）との間で、個人識別証明書（ＩＤＣ）の利用に関する運用規程を含む契約を行なう（Ｓ７１）。その後、個人識別認証局（ＩＤＡ）とサービスプロバイダ（ＳＰ）間での相互認証処理（Ｓ７２）を行なう。相互認証処理は、例えば共通鍵暗号方式、または公開鍵暗号方式に基づく処理として実行される。

【００８９】

相互認証処理が成立すると、サービスプロバイダ（ＳＰ）は、ＳＰのサービス提供予定のユーザ名あるいはユーザ識別データと、必要とする個人識別証明書（ＩＤＣ）のポリシーを個人識別証明書（ＩＤＣ）発行要求として個人識別認証局（ＩＤＡ）に送付する（Ｓ７３）。個人識別認証局（ＩＤＡ）は、発行要求を検証（Ｓ７４）し、運用規程に従って、個人識別証明書（ＩＤＣ）のポリシーを設定（Ｓ７５）し、要求のあったユーザの個人識別証明書（ＩＤＣ）をデータベースから抽出し、個人識別認証局（ＩＤＡ）の公開鍵で暗号化されているユーザ・テンプレートを復号した後、サービスプロバイダ（ＳＰ）の公開鍵で再暗号化（Ｓ７６）して、設定ポリシーに基づく個人識別証明書（ＩＤＣ）を生成（Ｓ７７）して、生成ＩＤＣをサービスプロバイダ（ＳＰ）に提供する（Ｓ７８）。なお、データベースに格納されたテンプレートが暗号化されていない場合、暗号化の要請がない場合は、テンプレートの暗号化処理は省略可能である。

【００９０】

（３．８．個人識別証明書（ＩＤＣ）更新）

次に、ユーザから提供され、登録されたテンプレートに基づいて生成される個人識別証明書（ＩＤＣ）の更新処理について説明する。更新処理は、主に使用している個人識別証明書（ＩＤＣ）に設定された有効期限の再設定処理として実行される。

【００９１】

図１６にサービスプロバイダ（ＳＰ）からの個人識別証明書（ＩＤＣ）更新要

求に対する処理の流れを示す。まず、個人識別証明書（ＩＤＣ）を利用しようとするサービスプロバイダは、個人識別認証局（ＩＤＡ）との間で、個人識別証明書（ＩＤＣ）の利用に関する運用規程を含む契約を行なう（Ｓ８１）。その後、個人識別認証局（ＩＤＡ）とサービスプロバイダ（ＳＰ）間での相互認証処理を行なう（Ｓ８２）。相互認証処理は、例えば共通鍵暗号方式、または公開鍵暗号方式に基づく処理として実行される。

【００９２】

相互認証処理が成立すると、サービスプロバイダ（ＳＰ）は、更新を必要とする個人識別証明書（ＩＤＣ）の更新要求を個人識別認証局（ＩＤＡ）に送付（Ｓ８３）する。個人識別認証局（ＩＤＡ）は、更新要求を検証（Ｓ８４）し、運用規程に従って、個人識別証明書（ＩＤＣ）のポリシーを設定（Ｓ８５）し、要求のあったユーザの個人識別証明書（ＩＤＣ）をデータベースから抽出し、個人識別認証局（ＩＤＡ）の公開鍵で暗号化されているユーザ・テンプレートを復号した後、サービスプロバイダ（ＳＰ）の公開鍵で再暗号化して、設定ポリシーに基づく個人識別証明書（ＩＤＣ）を生成（Ｓ８６）して、有効期間の設定を行ない、生成ＩＤＣをサービスプロバイダ（ＳＰ）に提供（Ｓ８７）する。なお、データベースに格納されたテンプレートが暗号化されていない場合、暗号化の要請がない場合は、テンプレートの暗号化処理は省略可能である。

【００９３】

（３．９．個人識別証明書（ＩＤＣ）削除）

次に、ユーザから提供され、登録されたテンプレートに基づいて生成される個人識別証明書（ＩＤＣ）の削除処理について説明する。

【００９４】

図１７にユーザからの個人識別証明書（ＩＤＣ）削除要求に対する処理の流れを示す。まず、個人識別証明書（ＩＤＣ）を削除しようとするユーザは、削除を必要とする個人識別証明書（ＩＤＣ）の削除要求を個人識別認証局（ＩＤＡ）に送付（Ｓ９１）する。個人識別認証局（ＩＤＡ）は、削除要求を検証（Ｓ９２）し、対応する個人識別証明書（ＩＤＣ）の削除を実行（Ｓ９３）する。

【００９５】

（３．１０．個人識別証明書（ＩＤＣ）照会）

次に、ユーザから提供され、登録されたテンプレートに基づいて生成される個人識別証明書（ＩＤＣ）の照会処理について説明する。照会処理は、例えばサービスプロバイダ（ＳＰ）が個人識別証明書（ＩＤＣ）を保有せず、ユーザから送付されたサンプリングデータを個人識別認証局（ＩＤＡ）に送付して、個人識別認証局（ＩＤＡ）にのおいて、個人識別認証局（ＩＤＡ）が保有する個人識別証明書（ＩＤＣ）に基づいて個人認証を行なって、その結果のみをサービスプロバイダ（ＳＰ）が利用するような場合に実行される処理である。

【００９６】

図１８にサービスプロバイダ（ＳＰ）からの個人識別証明書（ＩＤＣ）照会要求に対する処理の流れを示す。まず、個人識別証明書（ＩＤＣ）の照会を行なおうとするサービスプロバイダは、個人識別認証局（ＩＤＡ）との間で、個人識別証明書（ＩＤＣ）の利用に関する運用規程を含む契約を行なう（Ｓ０１）。その後、個人識別認証局（ＩＤＡ）とサービスプロバイダ（ＳＰ）間での相互認証処理を行なう（Ｓ０２）。相互認証処理は、例えば共通鍵暗号方式、または公開鍵暗号方式に基づく処理として実行される。

【００９７】

相互認証処理が成立すると、サービスプロバイダ（ＳＰ）は、照会を必要とする個人識別証明書（ＩＤＣ）の照会要求を個人識別認証局（ＩＤＡ）に送付するとともに、照会ユーザのサンプリングデータ等を送付（Ｓ０３，Ｓ０４））する。個人識別認証局（ＩＤＡ）は、照会要求を検証（Ｓ０５）し、受領サンプリングデータと個人識別証明書（ＩＤＣ）との照合（Ｓ０６）を行い、照合結果（ＯＫまたはＮＧ）をサービスプロバイダ（ＳＰ）に送付（Ｓ０７）する。

【００９８】

［４．個人識別証明書（ＩＤＣ）の基本的利用形態］

以下、個人識別証明書（ＩＤＣ）の基本的利用形態について、公開鍵証明書（ＰＫＣ）を発行する認証局（ＣＡ）と、個人識別証明書（ＩＤＣ）を発行する個人識別認証局（ＩＤＡ）と、これら各証明書を利用するデバイスとの関係を中心として説明する。

【００９９】

図１９および図２０に公開鍵証明書（ＰＫＣ）を発行する認証局（ＣＡ）と、個人識別証明書（ＩＤＣ）を発行する個人識別認証局（ＩＤＡ）と、これら各証明書を利用するデバイスの２つの構成例を示す。図１９の構成は、個人識別証明書（ＩＤＣ）のテンプレートとサンプリング情報との比較を個人識別認証局（ＩＤＡ）において実行する形態、図２０は、個人識別証明書（ＩＤＣ）のテンプレートとサンプリング情報との比較をサービスプロバイダ（ＳＰ）またはユーザデバイス（ＵＤ）において実行する形態における各システム構成を示している。

【０１００】

図１９のユーザデバイス（ＵＤ）またはサービスプロバイダ（ＳＰ）３００は、指紋データ等の様々な個人情報を取得し、処理するためのサンプリング情報処理部３１０を有し、サンプリング情報処理部３１０は、サンプリング情報を取得するための個人情報取得部３１４、指紋データ等のコード変換処理等を実行する情報変換部３１３、これらの変換コードを個人識別認証局３２０に送信する通信部３１２を有し、また、各種通信処理において暗号データ処理に使用する公開鍵証明書を格納している。制御部３１１は、個人情報取得部３１４、情報変換部３１３、通信部３１２における処理の制御を実行する。

【０１０１】

個人識別認証局（ＩＤＡ）３２０は、比較部３２１、記憶手段３２２を有し、比較部において記憶手段に格納された認証対象の各個人のテンプレート（個人識別証明書に格納され、暗号化されていることが望ましい）と、ユーザデバイス（ＵＤ）またはサービスプロバイダ（ＳＰ）３００から受信するサンプリング情報との比較（照合）を実行する。記憶手段には、テンプレートの他に個人識別証明書の発行履歴、照合処理履歴データが格納される。

【０１０２】

認証局（ＣＡ）３３０は、公開鍵証明書（ＰＫＣ）の発行機関であり、ユーザのリクエストに応じて、認証局の署名を付加したユーザの公開鍵証明書を発行する。認証局は、公開鍵証明書の発行履歴、照合処理履歴データを格納し、管理する。

【０１０３】

個人識別認証局（ＩＤＡ）３２０は、ユーザデバイス（ＵＤ）またはサービスプロバイダ（ＳＰ）３００からサンプリング情報を受信し、格納テンプレートとの比較を実行して、一致した場合には、結果通知としてＯＫまたはＮＧをユーザデバイス（ＵＤ）またはサービスプロバイダ（ＳＰ）３００に通知する。また、後述するが、所定のフォーマットに従った照合証明書を発行する構成としてもよい。個人識別認証局は、照合証明書を発行した場合は、発行履歴を格納する。

【０１０４】

認証局、（ＣＡ）、個人識別認証局（ＩＤＡ）３２０と、ユーザデバイス（ＵＤ）またはサービスプロバイダ（ＳＰ）３００との間の通信は、相互認証処理の成立を条件として実行され、機密データに関しては、相互認証において生成したセッションキーによる暗号化、あるいは、双方の公開鍵による暗号化を施して実行するのが望ましい。

【０１０５】

図２０は、個人識別証明書（ＩＤＣ）のテンプレートとサンプリング情報との比較をサービスプロバイダ（ＳＰ）またはユーザデバイス（ＵＤ）において実行する形態におけるシステム構成例である。

【０１０６】

図２０のユーザデバイス（ＵＤ）またはサービスプロバイダ（ＳＰ）４００は、指紋データ等の様々な個人情報を取得し、さらに照合処理を実行するための照合システム４１０を有し、照合システム４１０は、個人識別証明書を格納した一般メモリ４１３、個人識別証明書の改竄チェック処理を実行する個人識別証明書検証部４１４、個人識別証明書に格納された暗号化テンプレートの復号処理を実行するテンプレート復号化部４１５、指紋データ等のサンプリング情報を取得するための個人情報取得部４１８、指紋データ等のコード変換処理等を実行する情報変換部４１７、復号したテンプレートとコード化されたサンプリング情報とを比較する比較部４１６、個人識別認証局４２０とのデータ通信を実行する通信部４１１を有し、また、各種通信処理において暗号データ処理のための署名生成部、公開鍵証明書、秘密鍵を持つ暗号処理部４１９を有している。制御部４１２は

、各処理部における処理制御を実行する。

【０１０７】

個人識別認証局（ＩＤＡ）４２０は、個人識別証明書発行部４２１、記憶手段４２２を有し、認証対象の各個人のテンプレートを格納した個人識別証明書をユーザデバイス（ＵＤ）またはサービスプロバイダ（ＳＰ）４００からのリクエストに応じて発行する。記憶手段４２２には、テンプレート、個人識別証明書、個人識別証明書の発行履歴、照合処理履歴データが格納される。

【０１０８】

認証局（ＣＡ）４３０は、公開鍵証明書（ＰＫＣ）の発行機関であり、ユーザのリクエストに応じて、認証局の署名を付加したユーザの公開鍵証明書を発行する。認証局は、公開鍵証明書の発行履歴、照合処理履歴データを格納し、管理する。

【０１０９】

図１９の構成と同様、認証局、（ＣＡ）、個人識別認証局（ＩＤＡ）３２０と、ユーザデバイス（ＵＤ）またはサービスプロバイダ（ＳＰ）３００との間の通信は、相互認証処理の成立を条件として実行され、機密データに関しては、相互認証において生成したセッションキーによる暗号化、あるいは、双方の公開鍵による暗号化を施して実行するのが望ましい。

【０１１０】

［５．個人識別証明書（ＩＤＣ）を使用した認証処理態様］

次に、上述の個人識別証明書（ＩＤＣ）を用いた個人認証処理の様々な態様について説明する。個人識別証明書（ＩＤＣ）を用いた個人認証処理は、下記の２つのモードに大別される。

【０１１１】

（５．１．オンラインモード）

静的照合(Static IDC verification)

個人識別証明書（ＩＤＣ）のテンプレートは照合される場所、例えば個人識別認証局（ＩＤＡ）、サービスプロバイダ（ＳＰ）、あるいはユーザデバイス（ＰＣ）の公開鍵で暗号化されて個人識別認証局（ＩＤＡ）に登録、格納しており、

サービスプロバイダ（ＳＰ）、あるいはユーザデバイス（ＰＣ）からの要求に応じて個人識別認証局（ＩＤＡ）がＩＤＣを配布し、照合処理を実行する。

【０１１２】

動的照合(Dynamic IDC verification)

個人識別証明書（ＩＤＣ）のテンプレートは個人識別認証局（ＩＤＡ）の公開鍵で暗号化されてＩＤＡに登録されており、サービスプロバイダ（ＳＰ）、あるいはユーザデバイス（ＰＣ）からの要求に応じて照合される場所、すなわち個人認証処理実行エンティテイである例えばＳＰ、あるいはＰＣの公開鍵で暗号化し直し、動的に個人識別証明書（ＩＤＣ）を配布し照合処理が実行される。

【０１１３】

（５．２．オフラインモード）

静的照合

個人識別証明書（ＩＤＣ）のテンプレートは照合される場所、すなわち個人認証処理実行エンティテイである例えば個人識別認証局（ＩＤＡ）、サービスプロバイダ（ＳＰ）、あるいはユーザデバイス（ＰＣ）の公開鍵で暗号化、あるいは、テンプレートを共通鍵で暗号化し、該共通鍵を個人識別認証局（ＩＤＡ）、サービスプロバイダ（ＳＰ）、あるいはユーザデバイス（ＰＣ）の公開鍵で暗号化して個人識別認証局（ＩＤＡ）に登録され、各ユーザに配布されている。個人認証する際、照合先にＩＤＣとサンプリング情報を送り照合する。以下、上記の各モードにおける照合処理について説明する。

【０１１４】

（５．１．１．オンラインモード静的照合）

オンラインモード静的照合は、個人識別証明書（ＩＤＣ）のテンプレートと、各個人が入力したサンプリングデータとの照合処理の実行時に、個人識別認証局（ＩＤＡ）が動的に個人識別証明書（ＩＤＣ）を発行して、ユーザデバイス（ＰＣ）、サービスプロバイダ（ＳＰ）、個人識別認証局（ＩＤＡ）のいずれかのシステムにおいて照合処理を実行する形態であり、個人識別証明書（ＩＤＣ）のテンプレートと、各個人が入力したサンプリングデータとの照合処理を各システム、すなわち個人認証処理実行エンティテイにおいて実行する形態であり、個人識

別認証局（ＩＤＡ）は、照合処理を実行するシステムの公開鍵で暗号化されたテンプレート情報をデータベースから抽出して各システムに送付し、各システムにおいて受信ＩＤＣを復号して得られるテンプレートと、入力サンプリングデータとの照合を実行して個人識別を行なう構成である。

【０１１５】

図２１にユーザデバイス（例えばＰＣ）、サービスプロバイダ（ＳＰ）、個人識別認証局（ＩＤＡ）の各システムにおける照合処理の実行形態を説明する図を示す。なお、図２１（ａ）～（ｃ）におけるユーザデバイス、サービスプロバイダ（ＳＰ）、個人識別認証局（ＩＤＡ）等の各システム間におけるデータ転送は、基本的に各データ送受信システム間における相互認証処理が実行され、認証が成立したことを条件とし、認証処理において生成したセッションキーでデータの暗号化処理がなされて実行されるものである。

【０１１６】

図２１（ａ）は、ユーザデバイスにおいて照合処理を実行する形態である。個人識別認証局（ＩＤＡ）には、ユーザデバイスの公開鍵で暗号化されたテンプレートを格納した個人識別証明書（ＩＤＣ）が保管され、ユーザデバイスにおける照合処理の際には、ユーザデバイスから個人識別認証局（ＩＤＡ）に対して、個人認証の対象となる個人の個人識別証明書（ＩＤＣ）の取得要求を行なう。

【０１１７】

個人識別証明書（ＩＤＣ）の取得は、例えばその認証対象である個人またはユーザデバイスの公開鍵証明書（ＰＫＣ）の固有ＩＤを、ユーザデバイスから個人識別認証局（ＩＤＡ）に送信し、個人識別認証局（ＩＤＡ）が受信した固有ＩＤに基づいて格納ＩＤＣ中から対応する個人のＩＤＣを抽出してユーザデバイスに送信することにより実行される。公開鍵証明書（ＰＫＣ）と個人識別証明書（ＩＤＣ）とは、様々な態様のリンク構成が設定可能であり、設定されたリンク構成に応じたＩＤＣ識別データがユーザデバイスから個人識別認証局（ＩＤＡ）に送付され、個人識別認証局（ＩＤＡ）では、受信データをキーとして対応する個人識別証明書（ＩＤＣ）の抽出処理を実行する。なお、公開鍵証明書（ＰＫＣ）と個人識別証明書（ＩＤＣ）とのリンク態様については後段で詳細に説明する。

【０１１８】

ユーザデバイスは、個人識別認証局（ＩＤＡ）から受信した個人識別証明書（ＩＤＣ）中の暗号化テンプレートをユーザデバイスの秘密鍵で復号してテンプレートを取得し、サンプリング抽出装置において取得されたテンプレートに対応する個人データ、例えば指紋データ等のサンプリングデータとの照合を実行する。照合において一致すればＯＫであり、不一致であればＮＧとなる。ＩＤＣの格納テンプレートと、サンプリングデータとは対応する個人データ、すなわち指紋データであれば指紋データ、虹彩データであればいずれも虹彩データであることが必要である。なお、複数の異なる個人識別データをテンプレートとして個人識別証明書（ＩＤＣ）に格納し、そのいずれかと入力サンプリングデータとが一致すれば照合成立とする構成としてもよい。

【０１１９】

照合の成立を条件として、例えばその後のユーザデバイスに設定された特定のアプリケーションプログラムを実行し、データベースへのアクセス許可、あるいはデータ更新許可、データ入力許可、その他のデータ処理を実行可能とする。照合が不成立の場合は、データ処理の実行を不許可とする。この構成は、個人認証処理要求エンティテイおよび個人認証処理実行エンティテイが、照合処理機能を備えたデータ処理装置としてのユーザデバイスである。

【０１２０】

図２１（ｂ）は、サービスプロバイダ（ＳＰ）において照合処理を実行する形態である。個人識別認証局（ＩＤＡ）には、サービスプロバイダ（ＳＰ）の公開鍵で暗号化されたテンプレートを格納した個人識別証明書（ＩＤＣ）が保管され、サービスプロバイダ（ＳＰ）における照合処理の際には、ユーザデバイスから認証の実行対象となる個人のサンプリング情報と、その個人の公開鍵証明書（ＰＫＣ）が送信される。サービスプロバイダ（ＳＰ）がＰＫＣを既に保有している場合は、ＰＫＣを特定するための識別データでもよい。なお、サンプリングデータは、相互認証で生成したセッションキーで暗号化されるか、あるいは、サービスプロバイダ（ＳＰ）の公開鍵により暗号化され、サービスプロバイダ（ＳＰ）においてのみ復号可能な暗号化データとして送付することが好ましい。本構成は

、個人認証処理要求エンティテイはユーザデバイスであり、個人認証処理実行エンティテイは、該ユーザデバイスに対してサービスを提供するサービスプロバイダである。

【０１２１】

サービスプロバイダ（ＳＰ）は、個人またはユーザデバイスの公開鍵証明書（ＰＫＣ）の固有ＩＤを、ユーザデバイスから個人識別認証局（ＩＤＡ）に送信し、個人識別認証局（ＩＤＡ）に対して、個人認証の対象となる個人に対応する個人識別証明書（ＩＤＣ）の取得要求を行なう。個人識別認証局（ＩＤＡ）は受信した固有ＩＤに基づいて格納ＩＤＣ中から対応する個人のＩＤＣを抽出してサービスプロバイダ（ＳＰ）に送信する。このＩＤＣは、サービスプロバイダ（ＳＰ）の公開鍵で暗号化されたテンプレートを含むＩＤＣである。

【０１２２】

サービスプロバイダ（ＳＰ）は、個人識別認証局（ＩＤＡ）から受信した個人識別証明書（ＩＤＣ）中の暗号化テンプレートをサービスプロバイダ（ＳＰ）の秘密鍵で復号してテンプレートを取得し、サンプリング抽出装置において取得され、ユーザデバイスから送信された暗号化サンプリングデータ、例えば指紋データ等の暗号化サンプリングデータを復号したデータとの照合を実行する。照合において一致すればＯＫであり、不一致であればＮＧとなる。照合結果（ＯＫまたはＮＧ）は、ユーザデバイスに送信され、照合結果に応じて、その後の処理、例えばユーザデバイスからサービスプロバイダ（ＳＰ）に対するコンテンツの送付要求、あるいはデータ閲覧要求等のサービス実行の可否が決定される。

【０１２３】

図２１（ｃ）は、個人識別認証局（ＩＤＡ）において照合処理を実行する形態である。個人識別認証局（ＩＤＡ）には、個人識別認証局（ＩＤＡ）の公開鍵で暗号化されたテンプレートを格納した個人識別証明書（ＩＤＣ）が保管され、個人識別認証局（ＩＤＡ）における照合処理の際には、ユーザデバイスから認証の実行対象となる個人のサンプリング情報と、その個人またはユーザデバイスの公開鍵証明書（ＰＫＣ）がサービスプロバイダ（ＳＰ）を経由して個人識別認証局（ＩＤＡ）に送付される。個人識別認証局（ＩＤＡ）がＰＫＣを既に保有してい

る場合は、ＰＫＣを特定するための識別データでもよい。なお、サンプリングデータは、個人識別認証局（ＩＤＡ）の公開鍵により暗号化され、個人識別認証局（ＩＤＡ）においてのみ復号可能な暗号化データとして送付することが好ましい。本構成は、個人認証処理要求エンティテイはユーザデバイスまたはサービスプロバイダであり、個人認証処理実行エンティテイは個人識別認証局である。

【０１２４】

個人識別認証局（ＩＤＡ）は、個人の公開鍵証明書（ＰＫＣ）の固有ＩＤに基づいて格納ＩＤＣ中から対応する個人のＩＤＣを抽出して個人識別証明書（ＩＤＣ）中の暗号化テンプレートを個人識別認証局（ＩＤＡ）の秘密鍵で復号してテンプレートを取得し、サンプリング抽出装置において取得され、ユーザデバイスからサービスプロバイダ（ＳＰ）を経由して送信された暗号化サンプリングデータ、例えば指紋データ等の暗号化サンプリングデータを復号したデータとの照合を実行する。照合において一致すればＯＫであり、不一致であればＮＧとなる。照合結果（ＯＫまたはＮＧ）は、サービスプロバイダ（ＳＰ）および、ユーザデバイスに送信され、照合結果に応じて、その後の処理、例えばユーザデバイスからサービスプロバイダ（ＳＰ）に対するコンテンツの送付要求、あるいはデータ閲覧要求等のサービス実行の可否が決定される。

【０１２５】

（５．１．２オンラインモード動的照合）

オンラインモード動的照合は、個人識別証明書（ＩＤＣ）のテンプレートと、各個人が入力したサンプリングデータとの照合処理の実行時に、個人識別認証局（ＩＤＡ）が動的に個人識別証明書（ＩＤＣ）を発行して、ユーザデバイス（ＰＣ）、サービスプロバイダ（ＳＰ）、個人識別認証局（ＩＤＡ）のいずれかのシステムにおいて照合処理を実行する形態であり、個人識別認証局（ＩＤＡ）の公開鍵で暗号化されたテンプレート情報を、個人識別認証局（ＩＤＡ）において復号し、照合処理を実行する各システムの公開鍵で再暗号化したＩＤＣを各照合処理システムに送信して、各システムにおいて復号して得られるテンプレートと、入力サンプリングデータとの照合を実行して個人識別を行なう構成である。

【０１２６】

図２２は、ユーザデバイスにおいて照合処理を実行する形態である。個人識別認証局（ＩＤＡ）には、個人識別認証局（ＩＤＡ）の公開鍵で暗号化されたテンプレートを格納した個人識別証明書（ＩＤＣ）が保管され、ユーザデバイスにおける照合処理の際には、ユーザデバイスから個人識別認証局（ＩＤＡ）に対して、個人認証の対象となる個人の個人識別証明書（ＩＤＣ）の取得要求を行なう。

【０１２７】

個人識別証明書（ＩＤＣ）の取得は、例えばその認証対象である個人またはユーザデバイスの公開鍵証明書（ＰＫＣ）、または、個人識別認証局（ＩＤＡ）がすでにその個人またはユーザデバイスの公開鍵証明書（ＰＫＣ）を保有している場合は、公開鍵証明書（ＰＫＣ）の固有ＩＤを、ユーザデバイスから個人識別認証局（ＩＤＡ）に送信し、個人識別認証局（ＩＤＡ）が受信した固有ＩＤ、またはＰＫＣから取得した固有ＩＤに基づいて格納ＩＤＣ中から対応する個人のＩＤＣを抽出する。

【０１２８】

個人識別認証局（ＩＤＡ）は、抽出したＩＤＣの暗号化テンプレートを個人識別認証局（ＩＤＡ）の秘密鍵で復号し、さらに、ユーザデバイスの公開鍵で再暗号化を行ない、個人識別証明書（ＩＤＣ）を再発行し、再発行ＩＤＣをユーザデバイスに送信する。

【０１２９】

ユーザデバイスは、個人識別認証局（ＩＤＡ）から受信した個人識別証明書（ＩＤＣ）中の暗号化テンプレートをユーザデバイスの秘密鍵で復号してテンプレートを取得し、サンプリング抽出装置において取得されたテンプレートに対応する個人データ、例えば指紋データ等のサンプリングデータとの照合を実行する。照合において一致すればＯＫであり、不一致であればＮＧとなる。照合の成立を条件として、例えばその後のユーザデバイスに設定された特定のアプリケーションプログラムを実行し、データベースへのアクセス許可、あるいはデータ更新許可、データ入力許可、その他のデータ処理を実行可能とする。照合が不成立の場合は、データ処理の実行を不許可とする。

【０１３０】

図２３は、サービスプロバイダ（ＳＰ）において照合処理を実行する形態である。個人識別認証局（ＩＤＡ）には、個人識別認証局（ＩＤＡ）の公開鍵で暗号化されたテンプレートを格納した個人識別証明書（ＩＤＣ）が保管され、サービスプロバイダ（ＳＰ）における照合処理の際には、まず、サービスプロバイダ（ＳＰ）から個人識別認証局（ＩＤＡ）に対して、サービスプロバイダ（ＳＰ）の公開鍵証明書（ＰＫＣ）が送信される。個人識別認証局（ＩＤＡ）がサービスプロバイダ（ＳＰ）のＰＫＣを既に保有している場合は、ＰＫＣを特定するための識別データでもよい。

【０１３１】

次に、ユーザデバイスから認証の実行対象となる個人またはユーザデバイスの公開鍵証明書（ＰＫＣ）がサービスプロバイダ（ＳＰ）経由で、個人識別認証局（ＩＤＡ）に送信される。個人識別認証局（ＩＤＡ）がユーザデバイスのＰＫＣを既に保有している場合は、ＰＫＣを特定するための識別データでもよい。

【０１３２】

個人識別認証局（ＩＤＡ）は受信した固有ＩＤに基づいて格納ＩＤＣ中から対応する個人のＩＤＣを抽出して、抽出したＩＤＣの暗号化テンプレートを個人識別認証局（ＩＤＡ）の秘密鍵で復号し、さらに、サービスプロバイダ（ＳＰ）の公開鍵で再暗号化を行ない、個人識別証明書（ＩＤＣ）を再発行し、再発行ＩＤＣをサービスプロバイダ（ＳＰ）に送信する。

【０１３３】

サービスプロバイダ（ＳＰ）は、個人識別認証局（ＩＤＡ）から受信した個人識別証明書（ＩＤＣ）中の暗号化テンプレートをサービスプロバイダ（ＳＰ）の秘密鍵で復号してテンプレートを取得し、サンプリング抽出装置において取得され、ユーザデバイスから送信された暗号化サンプリングデータ、例えば指紋データ等の暗号化サンプリングデータを復号したデータとの照合を実行する。照合において一致すればＯＫであり、不一致であればＮＧとなる。照合結果（ＯＫまたはＮＧ）は、ユーザデバイスに送信され、照合結果に応じて、その後の処理、例えばユーザデバイスからサービスプロバイダ（ＳＰ）に対するコンテンツの送付要求、あるいはデータ閲覧要求等のサービス実行の可否が決定される。

【０１３４】

（５．２．オフラインモード）

オフラインモードでは、オンラインモードのように、サンプリング情報との照合時に、個人識別認証局（ＩＤＡ）が動的に個人識別証明書（ＩＤＣ）を発行する構成ではなく、静的照合のみである。したがって個人識別証明書（ＩＤＣ）に含まれるテンプレート情報の暗号方式、照合場所等により個人認証の実現方法が異なる。またオフラインモードでは個人識別証明書（ＩＤＣ）に含まれる暗号化テンプレートの復号を照合場所、例えばユーザデバイス、またはサービスプロバイダ（ＳＰ）で行なうため、ユーザデバイス、またはサービスプロバイダ（ＳＰ）において復号可能な暗号化を行なうことが必要である。

【０１３５】

オフラインでの静的照合の処理形態は以下のような場合に分類される。

（５．２．１）デバイスでの照合

ａ．個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）が同一デバイスに格納されたユーザデバイスの場合

ｂ．個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）が同一デバイスに格納されていないユーザデバイスの場合

（５．２．２）サービスプロバイダでの照合

ｃ．個人識別証明書（ＩＤＣ）のテンプレート情報がサービスプロバイダ（ＳＰ）の公開鍵で暗号化されている場合

ｄ．個人識別証明書（ＩＤＣ）のテンプレート情報がユーザデバイスの公開鍵、または共通鍵で暗号化されている場合

以下にそれぞれについて説明する。

【０１３６】

（５．２．１）デバイスでの照合

ａ．ＩＤＣとＰＫＣが同一デバイスに格納されたユーザデバイスの場合

ＩＤＣとＰＫＣが同一デバイスに格納されたユーザデバイスとは、個人識別証明書（ＩＤＣ）に含まれるテンプレートとサンプリング情報との照合処理を実行するユーザデバイスに、照合対象のユーザの個人識別証明書（ＩＤＣ）と公開鍵

証明書（ＰＫＣ）が存在し、その公開鍵証明書（ＰＫＣ）に含まれるデバイスの公開鍵によって個人識別証明書（ＩＤＣ）内のテンプレート情報が暗号化され、個人識別証明書（ＩＤＣ）から公開鍵証明書（ＰＫＣ）を特定可能な態様である。照合時には、個人識別証明書（ＩＤＣ）に含まれるテンプレートの暗号化方式、暗号鍵としての公開鍵を持つ公開鍵証明書（ＰＫＣ）を識別し、識別された公開鍵に対応する秘密鍵を特定し、秘密鍵によりテンプレートを復号する。

【０１３７】

図２４にＩＤＣとＰＫＣを格納したユーザデバイスにおける照合処理を説明する図を示す。ユーザデバイスは、サンプリング情報採取装置により採取された指紋情報等の個人データをサンプリング情報として入力し、さらに、ユーザデバイス内に格納された個人識別証明書（ＩＤＣ）を取り出し、テンプレート暗号化方式等の情報からテンプレート暗号化に適用された公開鍵の格納された公開鍵証明書（ＰＫＣ）を識別し、識別された公開鍵に対応する秘密鍵を特定する。秘密鍵は、ユーザデバイスの公開鍵、秘密鍵ペアの構成要素であり、ユーザデバイスのセキュアメモリに格納されているので、格納された秘密鍵により、個人識別証明書（ＩＤＣ）の暗号化テンプレートを復号する。次いで、復号したテンプレートと、サンプリング情報との照合処理を実行する。

【０１３８】

照合の成立を条件として、例えばその後のユーザデバイスに設定された特定のアプリケーションプログラムを実行し、データベースへのアクセス許可、あるいはデータ更新許可、データ入力許可、その他のデータ処理を実行可能とする。照合が不成立の場合は、データ処理の実行を不許可とする。

【０１３９】

ｂ．個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）が同一デバイスに格納されていないユーザデバイスの場合

多数のユーザが使用するデバイス（共有型ユーザデバイス）においては、ユーザそれぞれの個人識別証明書（ＩＤＣ）を格納することは困難である。このような場合、各ユーザの個人識別証明書（ＩＤＣ）を各個人端末（ｅｘ．ＩＣカード等のモバイル端末）からユーザデバイスに取り込み、取り込んだＩＤＣに基づい

て処理を行なうことになる。この処理形態は、さらに、以下の３つの態様に分類される。

（ｂ－１）個人端末格納のＩＤＣを共有型ユーザデバイスへ送信し照合

（ｂ－２）個人端末において復号したテンプレート情報を共有型ユーザデバイスへ送信し照合

（ｂ－３）個人端末側での照合処理

これらの処理について、以下説明する。

【０１４０】

（ｂ－１）個人端末格納のＩＤＣを共有型ユーザデバイスへ送信し照合

図２５に、例えばＩＣカード等の個人端末に格納された個人識別証明書（ＩＤＣ）を共有型ユーザデバイスへ送信して照合処理を実行する構成について説明する図を示す。

【０１４１】

共有型ユーザデバイスを用い、該共有ユーザデバイスに格納したアプリケーションプログラムにより、各種のデータ処理を実行しようとするそれぞれのユーザは、例えばＩＣカード等のモバイル端末を共有ユーザデバイスに装着する。ＩＣカードには、個人識別認証局（ＩＤＡ）が発行した個人識別証明書（ＩＤＣ）が格納されている。本構成では、共有ユーザデバイスが個人認証処理実行エンティテイである。

【０１４２】

ＩＣカード等のモバイル個人端末を共有ユーザデバイスに装着し、モバイル端末から個人識別証明書（ＩＤＣ）を共有ユーザデバイスに送信する。なお、ＩＤＣ送信に先立ち、モバイル端末と共有ユーザデバイスとの間での相互認証が実行され、ＩＤＣを相互認証時に生成したセッションキーで暗号化して送付する構成が望ましい。

【０１４３】

モバイル端末から個人識別証明書（ＩＤＣ）を受信した共有ユーザデバイスは、ＩＤＣに付加されている個人識別認証局（ＩＤＡ）の署名を検証し、ＩＤＣの改竄のないことを確認し、ＯＫ（改竄なし）の場合は、ＩＤＣから暗号化テンプ

レート情報を取り出す。なお、この暗号化テンプレートは、共有ユーザデバイスの公開鍵、あるいは共通鍵で暗号化されている。共有ユーザデバイスの公開鍵で暗号化されている場合は、共有ユーザデバイスの秘密鍵を用いて復号可能である。

【０１４４】

テンプレートが共通鍵で暗号化されている場合は、図２５の点線枠で示す処理を個人端末側で実行する。テンプレートを暗号化した共通鍵は、個人端末の公開鍵で暗号化して個人識別証明書（ＩＤＣ）に格納されている。個人端末は、個人識別証明書（ＩＤＣ）から暗号化共通鍵を取り出して、これを自己の秘密鍵で復号して共通鍵を取り出し、これを共有ユーザデバイスに送信する。なお、共通鍵は、相互認証時に生成したセッションキーで暗号化して送付する構成が望ましい。または、ユーザデバイスの公開鍵で共通鍵を暗号化して送付する構成としてもよい。

【０１４５】

共有ユーザデバイスは、自己の秘密鍵、または共通鍵を用いて暗号化テンプレートを復号し、サンプリング情報採取装置から入力されたサンプリング情報との照合を実行する。

【０１４６】

（ｂ－２）個人端末において復号したテンプレート情報を共有型ユーザデバイスへ送信し照合

図２６に、例えばＩＣカード等の個人端末に格納された個人識別証明書（ＩＤＣ）を復号した後、共有型ユーザデバイスへ送信して照合処理を実行する構成について説明する図を示す。

【０１４７】

ユーザは、ＩＣカード等のモバイル端末を共有ユーザデバイスに装着し、モバイル端末において復号した個人識別証明書（ＩＤＣ）を共有ユーザデバイスに送信する。ＩＤＣは、個々のユーザのモバイル端末に対応して設定された公開鍵で暗号化され、モバイル端末に対応して設定された秘密鍵で復号可能なテンプレート情報を含む構成である。ＩＤＣから抽出された暗号化テンプレート情報は、モ

バイル端末に対応して設定された秘密鍵により復号され、その後、ユーザデバイスに送信される。なお、テンプレート送信に先立ち、モバイル端末と共有ユーザデバイスとの間での相互認証を実行し、テンプレートを相互認証時に生成したセッションキーで暗号化して送付する構成が望ましい。または、ユーザデバイスの公開鍵でテンプレートを暗号化して送付する構成としてもよい。

【０１４８】

モバイル端末からテンプレートを受信した共有ユーザデバイスは、テンプレート情報を取り出し、サンプリング情報採取装置から入力されたサンプリング情報との照合を実行する。

【０１４９】

（ｂ－３）個人端末側での照合処理

図２７に、例えばＩＣカード等の個人端末に格納された個人識別証明書（ＩＤＣ）を用いて個人端末側で照合処理を実行して、その結果のみを共有型ユーザデバイスへ送信する構成について説明する図を示す。

【０１５０】

ユーザは、ＩＣカード等のモバイル端末を共有ユーザデバイスに装着し、モバイル端末において個人識別証明書（ＩＤＣ）の暗号化テンプレートの復号を実行する。ＩＤＣは、個々のユーザのモバイル端末に対応して設定された公開鍵で暗号化され、モバイル端末に対応して設定された秘密鍵で復号可能なテンプレート情報を含む構成である。ＩＤＣから抽出された暗号化テンプレート情報は、モバイル端末に対応して設定された秘密鍵により復号される。

【０１５１】

サンプリング情報は、サンプリング情報採取装置において採取され、その後、ユーザデバイスを介してＩＣカード等の個人端末に送信される。なお、サンプリング情報転送に先立ち、モバイル端末と共有ユーザデバイスとの間での相互認証を実行し、サンプリング情報を相互認証時に生成したセッションキーで暗号化して送付する構成が望ましい。ユーザデバイスからサンプリング情報を受信した個人端末は、復号したテンプレートとサンプリング情報との照合を実行し、その結果をユーザデバイスに送信する。本構成では、モバイル端末であるＩＣカードが

個人認証処理実行エンティテイである。

【０１５２】

（５．２．２）サービスプロバイダでの照合

次に、サービスプロバイダ（ＳＰ）における様々なサービス提供に際しての個人認証処理をサービスプロバイダにおいて実行する処理形態について説明する。

【０１５３】

ｃ．個人識別証明書（ＩＤＣ）のテンプレート情報がサービスプロバイダ（ＳＰ）の公開鍵で暗号化されている場合

まず、個人識別証明書（ＩＤＣ）のテンプレート情報がサービスプロバイダ（ＳＰ）の公開鍵で暗号化されている場合の処理について、図２８を用いて説明する。

【０１５４】

サービスプロバイダ（ＳＰ）の提供するサービス、例えばコンテンツ配信、決済等のサービスを受けようとするユーザデバイスは、まず、サンプリング情報採取装置により個人の指紋データ等のサンプリング情報を取得する。次に、ユーザデバイスは、サービスプロバイダ（ＳＰ）との間で相互認証処理を実行し、認証成立を条件としてサンプリング情報をサービスプロバイダ（ＳＰ）に送信する。サンプリング情報は、相互認証時に生成したセッションキー、または、サービスプロバイダの公開鍵による暗号化を施して送信する。さらに、ユーザデバイスは、自己の個人識別証明書（ＩＤＣ）をサービスプロバイダに送信する。この個人識別証明書（ＩＤＣ）には、サービスプロバイダの公開鍵による暗号化の施されたテンプレート情報が格納されている。

【０１５５】

ユーザデバイスからサンプリング情報と、個人識別証明書（ＩＤＣ）とを受信したサービスプロバイダ（ＳＰ）は、個人識別証明書（ＩＤＣ）に格納された暗号化テンプレート情報を自己（ＳＰ）の秘密鍵を用いて復号し、これとサンプリング情報との照合処理を実行する。

【０１５６】

照合が成立した場合は、個人認証が成立したとみなされ、そのサービスプロバ

イダの提供する例えばコンテンツ配信、決済処理等の各種サービスをユーザ（ユーザデバイス）に対して実行する。照合不成立である場合は、個人認証が不成立とみなされ、サービス提供の実行を停止する。

【０１５７】

ｄ．個人識別証明書（ＩＤＣ）のテンプレート情報がユーザデバイスの公開鍵、または共通鍵で暗号化されている場合

次に、個人識別証明書（ＩＤＣ）のテンプレート情報がユーザデバイスの公開鍵、または共通鍵で暗号化されている場合のサービスプロバイダ（ＳＰ）における個人認証について説明する。この場合の処理形態は、以下の３形態に分類される。

（ｄ－１）ユーザデバイスによりテンプレートの暗号化に使用した共通鍵をサービスプロバイダ（ＳＰ）に送信して照合する場合、

（ｄ－２）ユーザデバイスにおいて復号したテンプレート情報をサービスプロバイダ（ＳＰ）に送信して照合する場合、

（ｄ－３）ユーザデバイス側での照合処理

これらの処理について、以下説明する。

【０１５８】

（ｄ－１）ユーザデバイス格納のＩＤＣを共有型ユーザデバイスへ送信し照合

図２９に、ユーザデバイスに格納された個人識別証明書（ＩＤＣ）をサービスプロバイダ（ＳＰ）へ送信して照合処理を実行する構成について説明する図を示す。

【０１５９】

サービスプロバイダ（ＳＰ）のサービスを受けようとするユーザデバイスのユーザは、まず、サービスプロバイダ（ＳＰ）との間で相互認証処理を実行し、認証成立を条件として自己の個人識別証明書（ＩＤＣ）をサービスプロバイダに送信する。なお、ＩＤＣは相互認証時に生成したセッションキー、あるいはサービスプロバイダ（ＳＰ）の公開鍵で暗号化して送付する構成が望ましい。

【０１６０】

ユーザデバイスから個人識別証明書（ＩＤＣ）を受信したサービスプロバイダ

（ＳＰ）は、ＩＤＣに付加されている個人識別認証局（ＩＤＡ）の署名を検証し、ＩＤＣの改竄のないことを確認し、ＯＫ（改竄なし）の場合は、ＩＤＣから暗号化テンプレート情報を取り出す。なお、この暗号化テンプレートは共通鍵で暗号化されている。

【０１６１】

テンプレートを暗号化した共通鍵は、ユーザデバイスの公開鍵で暗号化して個人識別証明書（ＩＤＣ）に格納されている。ユーザデバイスは、個人識別証明書（ＩＤＣ）から暗号化共通鍵を取り出して、これを自己の秘密鍵で復号して共通鍵を取り出し、これをサービスプロバイダ（ＳＰ）に送信する。なお、共通鍵は、相互認証時に生成したセッションキーで暗号化して送付する構成が望ましい。または、サービスプロバイダ（ＳＰ）の公開鍵で共通鍵を暗号化して送付する構成としてもよい。

【０１６２】

サービスプロバイダ（ＳＰ）は、自己の秘密鍵、またはセッションキーで復号して共通鍵を取得し、取得した共通鍵を用いて暗号化テンプレートを復号し、サンプリング情報採取装置から入力され、ユーザデバイスを介して送付されたサンプリング情報との照合を実行する。ユーザデバイスは、サービスプロバイダ（ＳＰ）との間で相互認証処理を実行し、認証成立を条件としてサンプリング情報をサービスプロバイダ（ＳＰ）に送信する。サンプリング情報は、相互認証時に生成したセッションキー、または、サービスプロバイダの公開鍵による暗号化を施して送信する。

【０１６３】

（ｄ－２）ユーザデバイスにおいて復号したテンプレート情報をサービスプロバイダ（ＳＰ）へ送信し照合

図３０に、ユーザデバイスに格納された個人識別証明書（ＩＤＣ）を復号した後、サービスプロバイダ（ＳＰ）へ送信して照合処理を実行する構成について説明する図を示す。

【０１６４】

ユーザは、ユーザデバイスにおいて復号した個人識別証明書（ＩＤＣ）をサー

ビスプロバイダ（ＳＰ）に送信する。ＩＤＣは、個々のユーザデバイスに対応して設定された公開鍵で暗号化され、ユーザデバイスに対応して設定された秘密鍵で復号可能なテンプレート情報を含む構成である。ＩＤＣから抽出された暗号化テンプレート情報は、ユーザデバイスに対応して設定された秘密鍵により復号され、その後、サービスプロバイダ（ＳＰ）に送信される。なお、テンプレート送信に先立ち、ユーザデバイスとサービスプロバイダ（ＳＰ）との間での相互認証を実行し、テンプレートを相互認証時に生成したセッションキーで暗号化して送付する構成が望ましい。または、サービスプロバイダ（ＳＰ）の公開鍵でテンプレートを暗号化して送付する構成としてもよい。

【０１６５】

ユーザデバイスからテンプレートを受信したサービスプロバイダ（ＳＰ）は、テンプレート情報を取り出し、サンプリング情報採取装置から入力され、ユーザデバイスを介して受信したサンプリング情報との照合を実行する。

【０１６６】

（ｂ－３）ユーザデバイス側での照合処理

図３１に、ユーザデバイスに格納された個人識別証明書（ＩＤＣ）を用いてユーザデバイス側で照合処理を実行して、その結果のみをサービスプロバイダ（ＳＰ）へ送信する構成について説明する図を示す。

【０１６７】

ユーザデバイスは、個人識別証明書（ＩＤＣ）の暗号化テンプレートの復号を実行する。ＩＤＣは、個々のユーザデバイスに対応して設定された公開鍵で暗号化され、ユーザデバイスに対応して設定された秘密鍵で復号可能なテンプレート情報を含む構成である。ＩＤＣから抽出された暗号化テンプレート情報は、ユーザデバイスに対応して設定された秘密鍵により復号される。

【０１６８】

サンプリング情報は、サンプリング情報採取装置において採取され、その後、ユーザデバイスに入力されて、復号したテンプレートとサンプリング情報との照合を実行し、その結果をサービスプロバイダ（ＳＰ）に送信する。サービスプロバイダ（ＳＰ）は、結果に基づいてサービスの提供の可否を決定する。

【０１６９】

［６．個人識別証明書に基づくユーザ認証によるコンテンツの利用権制御処理］

次に、音楽データ、画像データ、ゲーム等の各種プログラム等、様々なコンテンツの利用において、個人識別証明書（ＩＤＣ）に基づいてユーザ認証を実行することにより、コンテンツ利用権を制御する処理構成について説明する。

【０１７０】

図３２にコンテンツ取り引きにおいて流通するコンテンツを含むセキュア・コンテナ（Ｓｅｃｕｒｅ　Ｃｏｎｔａｉｎｅｒ）の構成を示す。サービスプロバイダからユーザデバイスに対するコンテンツ配信、さらに、ユーザデバイスから他のユーザデバイスに対するコンテンツ配信においても図３２に示すセキュアコンテナを流通させる。

【０１７１】

なお、セキュアコンテナは、サービスプロバイダからユーザに配信されるばかりでなく、ユーザ間配信が可能である。ユーザ間コンテンツ配信の形態にはさらに２つの形態がある。１つは、ユーザＡからユーザＢ、さらにユーザＢからユーザＣ等、直列的に異なるユーザ間をコンテンツが順次、取り引きされる形態である。この直列的なユーザ間のコンテンツ配信が「世代間配信」である。もう１つの配信形態は、ユーザＡの購入したコンテンツをユーザＡからユーザＢ，Ｃ，Ｄ等、並列的に配信する形態である。すなわち１人のユーザから複数のユーザに並列に同一コンテンツを配信する形態である。この並列的なコンテンツ配信が「二次配信」である。

【０１７２】

図３２に示すようにセキュアコンテナ７００は、コンテンツ鍵によって暗号化されたコンテンツ７０１と、コンテンツの料金とコンテンツ料金の受け取り先、配分情報を含む価格情報７０２と、コンテンツの利用条件、例えば「世代間配信」「二次配信」等の転売が禁止されている１回限りの配信が許容されたコンテンツであるとか、複数回の転売が可能であるとか、複数回の転売が可能である場合の転売条件、例えば２回までの「世代間配信」と、３回までの「二次配信」が許

容されているコンテンツであるとか、あるいは利用可能期間等の設定情報としての販売条件（ＵＣＰ）７０３と、セキュアコンテナの作成者、例えばサービスプロバイダの電子署名７０４を含んで構成される。セキュアコンテナの価格情報７０２、販売条件（ＵＣＰ）７０３をコンテナ情報と総称する。セキュアコンテナのコンテナ情報である価格情報７０２、販売条件（ＵＣＰ）７０３の少なくともいずれか、あるいは両者にはコンテンツ利用の許可されたユーザの個人識別証明書（ＩＤＣ）のリストが含まれる。

【０１７３】

図３３に個人識別証明書（ＩＤＣ）のリスト構成を示す。個人識別証明書（ＩＤＣ）のリストには、ユーザの識別子であるユーザＩＤ、および各ユーザに対応する個人識別証明書（ＩＤＣ）の識別子がデータとして含まれる。

【０１７４】

コンテナ情報である価格情報７０２、販売条件（ＵＣＰ）７０３は、コンテンツ製作者、コンテンツプロバイダ、サービスプロバイダ等のいずれかが設定する管理データである。例えばサービスプロバイダは、予めユーザ登録をしているユーザの個人識別証明書（ＩＤＣ）のリストを価格情報７０２、販売条件７０３等に含めて各データを生成する。電子署名は、コンテンツの流通を管理する機関による署名である。コンテンツの流通を管理する機関がサービスプロバイダであれば、サービスプロバイダの署名となる。

【０１７５】

図３４に販売条件（ＵＣＰ）７０３の具体的構成例を示す。図３４に示すように販売条件（ＵＣＰ）には、コンテンツの利用可能なユーザの個人識別証明書（ＩＤＣ）の識別子をリスト化したデータである個人識別証明書（ＩＤＣ）リスト７１１を含む。さらに、コンテンツ識別子（ＩＤ）、コンテンツの利用可能なユーザデバイスを設定した使用可能機器条件、コンテンツの利用可能な地域を設定した地域コード、どのようにコンテンツを利用してよいかを示す利用権タイプ（例えばコンテンツの再生可能回数、コンテンツの複製（ダウンロード）可能回数）が含まれる。

【０１７６】

利用権タイプは、コンテンツの利用権を設定したデータである。図３５に利用権データの構成例を示す。ルール番号に対応付けて、利用権の内容、例えばコンテンツの再生権、複製（コピー）権、さらにそれぞれの権利期間、回数等が設定されている。なお、図中のＳＣＭＳはコピー回数等を設定したコピー制御情報である。ユーザは、セキュアコンテナの販売条件に設定されたルール番号により指定される利用権の範囲でコンテンツの再生、複製が許容される。

【０１７７】

さらに、図３４に示す販売条件（ＵＣＰ）には、異なるユーザデバイス間での流通可能回数として、「世代間配信」の可能回数を設定した「ＵＣＰ世代管理情報」７１２と、「二次配信」の可能回数を設定した「二次配信可能回数」７１３が含まれている。「ＵＣＰ世代管理情報」に設定されたユーザ間配信可能回数は、セキュアコンテナの利用に応じてユーザデバイス内のメモリに格納される使用制御情報（ＵＣＳ：Usage Control Status）（図３８参照）に引き継がれる。「ＵＣＰ世代管理情報」に設定されたユーザ間配信可能回数は、使用制御情報（ＵＣＳ）中の「ＵＣＳ世代管理情報」、「ＵＣＳ二次配信可能回数」の元データとなり、「ＵＣＳ世代管理情報」、「ＵＣＳ二次配信可能回数」に基づいてコンテンツ処理の可否が決定される。「ＵＣＳ世代管理情報」はコンテンツの世代間配信毎に更新され、「ＵＣＳ二次配信可能回数」はコンテンツの二次配信毎に更新される。使用制御情報（ＵＣＳ：Usage Control Status）については後段で説明する。

【０１７８】

図３６は、セキュアコンテナに含まれる価格情報のデータ構成例を示すものであり、図３４の販売条件（ＵＣＰ）と同様のコンテンツＩＤ等の情報の他に、価格情報ＩＤ、価格情報バージョンが含まれる。さらに、図３４の販売条件（ＵＣＰ）と同様、個人識別証明書（ＩＤＣ）リスト７２１を含む。すなわちコンテンツの利用可能なユーザの個人識別証明書（ＩＤＣ）の識別子をリスト化したデータを含む。

【０１７９】

図３７にセキュアコンテナを利用したコンテンツの配信処理形態を示す。コ

ンテンツプロバイダ（ＣＰ）８０１がセキュアコンテナに格納するコンテンツを生成、または取得し、コンテンツと、そのコンテンツの販売条件（ＵＣＰ）データをコンテンツのユーザに対する配信を行なうサービスプロバイダ（ＳＰ）８０２に提供する。サービスプロバイダ（ＳＰ）８０２は、コンテンツの利用に対する価格情報を生成して、価格情報、販売条件（ＵＣＰ）の少なくともいずれか、あるいは両者にコンテンツ利用の許可されたユーザの個人識別証明書（ＩＤＣ）のリストを格納し、電子署名を行なってセキュアコンテナを形成し、ユーザデバイス８０３に送付する。

【０１８０】

ユーザデバイス８０３は、セキュアコンテナの署名検証を行なう。さらに、セキュアコンテナの各構成データである販売条件（ＵＣＰ）データ、価格情報等の署名検証を行ない、各データの改竄チェックを実行し、さらに、販売条件（ＵＣＰ）データ、価格情報のいずれかの個人識別証明書（ＩＤＣ）リストから、自己のＩＤＣ識別子を抽出し、ＩＤＣ識別子によって特定される個人識別証明書（ＩＤＣ）を取得して、ＩＤＣ内のテンプレートとサンプリング情報との照合を実行する。なお照合処理は、ユーザデバイス、サービスプロバイダ、個人識別認証局（ＩＤＡ）のいずれかにおいて実行する。この個人認証の成立を条件として、コンテンツの利用、すなわちコンテンツの復号が実行可能となる。具体的には、照合成立を条件としてコンテンツの暗号化に使用しているコンテンツ鍵をサービスプロバイダからユーザデバイスに送信する。ユーザデバイスは、コンテンツ鍵を利用してセキュアコンテナのコンテンツの復号、再生が可能となる。

【０１８１】

ユーザデバイスは、さらに、セキュアコンテナをユーザデバイス８０３の記憶媒体に格納し、コンテンツ利用に際し発生する利用料金を課金情報として生成し、決済処理を行なうクリアリングセンタ８０４に送信する。課金情報は、前述の価格情報に設定されたデータに基づいて生成される。クリアリングセンタでは、課金情報に基づいて例えばユーザの電子マネー口座からの金額振替処理を実行する。ユーザデバイス８０３は、さらに他のユーザデバイス８０５に対してセキュアコンテナを流通させることができる。この態様については後述する。なお、ユ

ーザデバイス８０３，８０５は、セキュアコンテナの格納に際し、使用制御情報（ＵＣＳ）を生成してメモリに格納する。

【０１８２】

図３８にセキュアコンテナ格納に応じてユーザデバイスにおいて生成されユーザデバイス内のメモリに格納される使用制御情報（ＵＣＳ：Usage Control Status）の例を示す。図３８に示すように、使用制御情報（ＵＣＳ）には、コンテンツＩＤ、サービスプロバイダＩＤ等の情報の他に、再生残り回数、複製残り回数等のコンテンツ利用の制限情報が含まれる。これら、再生残り回数、複製残り回数は、同一のユーザデバイス内で利用可能な再生残り回数、複製残り回数を示すデータである。これらは、コンテンツの販売条件（ＵＣＰ）データに含まれるコンテンツの利用権を設定した利用権データに基づいて生成され、更新、継承されるデータである。従って、ユーザデバイスは、コンテンツ利用権の設定情報であるコンテンツの販売条件（ＵＣＰ）データに含まれるコンテンツ利用権データ、あるいは利用権データに基づいて生成される使用制御情報に従ってコンテンツの利用を実行することになる。

【０１８３】

使用制御情報（ＵＣＳ）には、さらに、個人識別証明書（ＩＤＣ）リスト７３１を含む。すなわちコンテンツの利用可能なユーザの個人識別証明書（ＩＤＣ）の識別子をリスト化したデータを含む。このリストは、販売条件（ＵＣＰ）に設定されたデータを継承したデータである。さらに、使用制御情報（ＵＣＳ）には、「ＵＣＳ世代管理情報」７３２、および「ＵＣＳ二次配信可能回数」７３３が含まれる。

【０１８４】

「ＵＣＳ世代管理情報」は前述したように、「世代間配信」の可能回数を設定したものであり、コンテンツを最初に購入したユーザデバイスは、販売条件（ＵＣＰ）中の「ＵＣＰ世代管理情報」に一致する回数が設定され、ユーザからの世代間配信によってコンテンツを受領したユーザデバイスは、同一セキュアコンテナについてすでに実行された世代間配信の回数が減じられた回数が設定される。

【０１８５】

「ＵＣＳ二次配信可能回数」７３３は前述の「二次配信」の可能回数を設定したフィールドであり、コンテンツを最初に購入したユーザデバイスは、販売条件（ＵＣＰ）中の「ＵＣＰ二次配信可能回数」に一致する回数が設定され、その後の二次配信に応じて更新、すなわち設定回数がデクリメントされる。

【０１８６】

このように、コンテンツのユーザ間での配信は、ユーザデバイス内のメモリにコンテンツに応じて格納される使用制御情報（ＵＣＳ：Usage Control Status）中の「ＵＣＳ世代管理情報」、「ＵＣＳ二次配信可能回数」に基づいて、それぞれの処理の可否が決定される。「ＵＣＳ世代管理情報」はコンテンツの世代間配信毎に更新され、「ＵＣＳ二次配信可能回数」はコンテンツの二次配信毎に更新される。

【０１８７】

図３９にコンテンツを格納したセキュアコンテナをサービスプロバイダからユーザデバイスに配信する際の個人識別証明書（ＩＤＣ）の利用を説明する図を示す。

【０１８８】

ユーザデバイス８１０のユーザ８２０は、まず自己の個人識別証明書（ＩＤＣ）の発行を個人識別認証局（ＩＤＡ）８３０に依頼する。この際、ユーザは、個人の生体情報、その他の個人情報を提供する。個人識別認証局（ＩＤＡ）８３０は、ユーザの正当性を確認した上で、サンプリング情報に基づくテンプレート情報を生成し、テンプレート情報を暗号化して格納した個人識別証明書（ＩＤＣ）を生成する。

【０１８９】

生成した個人識別証明書（ＩＤＣ）は要求に応じて、ユーザデバイス８１０、あるいはサービスプロバイダ８４０に配信され、格納される。ユーザ８２０が例えばサービスプロバイダ８４０からのコンテンツ配信を受ける際、ユーザの個人認証手続きをサービスプロバイダ８４０の有する個人識別証明書（ＩＤＣ）に基づいて実行する。すなわち、ユーザの提供するサンプリング情報と、個人識別証明書（ＩＤＣ）内のテンプレート情報とを照合して一致した場合は、サンプリン

グ情報を提供したユーザが個人識別証明書（ＩＤＣ）に対応する正当なユーザであると判定して、コンテンツ配信を実行する。

【０１９０】

また、ユーザデバイス８１０の使用の際にも、ユーザデバイス８１０に格納した個人識別証明書（ＩＤＣ）に基づいてユーザの個人認証手続きを実行する。すなわち、ユーザの入力するサンプリング情報と、個人識別証明書（ＩＤＣ）内のテンプレート情報とを照合して一致した場合は、サンプリング情報を提供したユーザが個人識別証明書（ＩＤＣ）に対応する正当なユーザであると判定して、ユーザデバイスを使用したデータ処理を実行可能とする。

【０１９１】

このように個人識別証明書（ＩＤＣ）を使用した個人認証処理は、様々な場所、すなわちユーザデバイスやサービスプロバイダにおいて独自に実行することができる。なお、前述したように、個人識別証明書（ＩＤＣ）内のテンプレートは、照合処理を実行するシステムの公開鍵で暗号化して格納されている。

【０１９２】

図４０にセキュアコンテナをサービスプロバイダから受領し、ユーザデバイスにおいて個人認証処理を実行して、正当なユーザにのみコンテンツ利用を可能とした処理フローを示す。以下、フローの各ステップについて説明する。

【０１９３】

ステップＳ７０１では、サービスプロバイダとユーザデバイス間で相互認証を実行し、認証成立を条件（Ｓ７０２でＹｅｓ）として、サービスプロバイダは、セキュアコンテナを抽出し（Ｓ７０３）、ユーザデバイスに送信する（Ｓ７０４）。なお、相互認証時にセッションキーが生成され、以下のサービスプロバイダとユーザデバイス間でのデータ転送は、必要に応じてセッションキーでの暗号化処理が行なわれる。

【０１９４】

ユーザデバイスは受信したセキュアコンテナの検証を行なう（Ｓ７０５）、検証には、セキュアコンテナ自体の署名検証、コンテナ内の価格情報、販売条件情報（ＵＣＰ）等の個別データの署名検証処理を含む。

【０１９５】

コンテナ検証が成功すると（Ｓ７０６，Ｙｅｓ）、ユーザは、サンプリング情報とユーザＩＤをユーザデバイスに入力（Ｓ７０７）し、ユーザデバイスは、セキュアコンテナの価格情報、販売条件情報（ＵＣＰ）のいずれかから個人識別証明書（ＩＤＣ）リストを抽出し（Ｓ７０８）、ユーザＩＤに基づいて対応するＩＤＣ識別子を検索する（Ｓ７０９）。入力ユーザＩＤに対応するＩＤＣ識別子が検出されない場合は、サービスプロバイダの認めたユーザでないと判定され、エラーとなり（Ｓ７１０でＮｏ）、処理は続行されない。

【０１９６】

個人識別証明書（ＩＤＣ）リストに入力ユーザＩＤに対応するＩＤＣ識別子が検出された場合（Ｓ７１０でＹｅｓ）は、ＩＤＣ識別子に基づいて個人識別証明書（ＩＤＣ）を取得（Ｓ７１１）する。個人識別証明書（ＩＤＣ）は、ユーザデバイスに格納されている場合は、ユーザデバイスに格納されたＩＤＣを用い、ない場合は、個人識別認証局（ＩＤＡ）、またはサービスプロバイダから取り寄せる。取得した個人識別証明書（ＩＤＣ）からテンプレートを取り出して、自己の秘密鍵で復号し、テンプレートとサンプリング情報との照合を実行し（Ｓ７１２）、照合が成立しない場合（Ｓ７１３でＮｏ）は、エラーとなり、その後の処理が続行されない。具体的にはコンテンツの復号処理が実行されず、コンテンツの利用が制限される。照合が成立した場合（Ｓ７１３でＹｅｓ）は、照合成立がサービスプロバイダに通知され、サービスプロバイダはセキュアコンテナに格納された暗号化コンテンツの復号に適用するコンテンツ鍵をユーザデバイスに送信する（Ｓ７１４）。ユーザデバイスでは、サービスプロバイダから受信したコンテンツ鍵を使用して暗号化コンテンツの復号を行ないコンテンツを利用（Ｓ７１５）する。

【０１９７】

このように、個人識別証明書（ＩＤＣ）のテンプレートを用いたユーザの個人識別処理を実行し、照合成立により、正当ユーザであることが確認された場合にのみセキュアコンテナに格納されたコンテンツの利用を可能とする構成により、不当なユーザのコンテンツ利用を防止することが可能となる。

【０１９８】

次に、図４１にサービスプロバイダにおいて個人認証処理を実行して、正当なユーザにのみセキュアコンテナを配信する処理フローを示す。以下、フローの各ステップについて説明する。

【０１９９】

ステップＳ７２１では、サービスプロバイダとユーザデバイス間で相互認証を実行する。相互認証時にセッションキーが生成され、以下のサービスプロバイダとユーザデバイス間でのデータ転送は、必要に応じてセッションキーでの暗号化処理が行なわれる。

【０２００】

相互認証成立を条件（Ｓ７２２でＹｅｓ）として、サービスプロバイダは、セキュアコンテナを抽出し（Ｓ７２３）、ユーザデバイスは、サンプリング情報とユーザＩＤをユーザデバイスに入力（Ｓ７３５）し、これらをサービスプロバイダに送信（Ｓ７３６）する。

【０２０１】

サービスプロバイダは、セキュアコンテナの価格情報、販売条件情報（ＵＣＰ）のいずれかから個人識別証明書（ＩＤＣ）リストを抽出し（Ｓ７２４）、ユーザＩＤに基づいて対応するＩＤＣ識別子を検索する（Ｓ７２５）。入力ユーザＩＤに対応するＩＤＣ識別子が検出されない場合は、サービスプロバイダの認めたユーザでないこととなり、エラーとなり（Ｓ７２６でＮｏ）、処理は続行されない。

【０２０２】

個人識別証明書（ＩＤＣ）リストに入力ユーザＩＤに対応するＩＤＣ識別子が検出された場合（Ｓ７２６でＹｅｓ）は、ＩＤＣ識別子に基づいて個人識別証明書（ＩＤＣ）を取得（Ｓ７２７）する。個人識別証明書（ＩＤＣ）は、サービスプロバイダに格納されている場合は、サービスプロバイダに格納されたＩＤＣを用い、ない場合は、個人識別認証局（ＩＤＡ）から取り寄せる。取得した個人識別証明書（ＩＤＣ）からテンプレートを取り出して、自己の秘密鍵で復号し、テンプレートとサンプリング情報との照合を実行し（Ｓ７２８）、照合が成立しな

い場合（Ｓ７２９でＮｏ）は、エラーとなり、その後の処理が続行されない。具体的にはセキュアコンテナの配信が実行されない。照合が成立した場合（Ｓ７２９でＹｅｓ）は、正当なユーザであると判定され、その後の処理が続行される。具体的にはサービスプロバイダからユーザデバイスに対するセキュアコンテナ、およびコンテンツ鍵の配信が実行される（Ｓ７３０）。

【０２０３】

サービスプロバイダは、セキュアコンテナをユーザデバイスに送信し、ユーザデバイスは受信したセキュアコンテナの検証を行なう（Ｓ７３１）、検証には、セキュアコンテナ自体の署名検証、コンテナ内の価格情報、販売条件情報（ＵＣＰ）等の個別データの署名検証処理を含む。コンテナ検証が成功すると（Ｓ７３２，Ｙｅｓ）、ユーザデバイスにおいてセキュアコンテナのコンテンツ利用が可能となる。

【０２０４】

このように、サービスプロバイダ側で、個人識別証明書（ＩＤＣ）のテンプレートを用いたユーザの個人識別処理を実行し、照合成立により、正当ユーザであることが確認された場合にのみセキュアコンテナの配信を実行する構成により、不当なユーザに対するコンテンツ配信を防止することが可能となる。

【０２０５】

次に、ユーザデバイス間におけるセキュアコンテナの配信処理における個人識別証明書（ＩＤＣ）の利用形態について説明する。

【０２０６】

図４２にセキュアコンテンナを利用したコンテンツのユーザ間の配信処理形態を示す。サービスプロバイダ（ＳＰ）は、コンテンツの利用に対する価格情報を生成して、価格情報、販売条件（ＵＣＰ）の少なくともいずれか、あるいは両者にコンテンツ利用の許可されたユーザの個人識別証明書（ＩＤＣ）のリストを格納し、電子署名を行なってセキュアコンテナを形成し、ユーザデバイス１，９２０に送付する。

【０２０７】

ユーザデバイス１，９２０の利用を行なうユーザ９４０，９４５は、正当なコ

ンテンツの利用が認められたユーザである場合、コンテンツに対応するセキュアコンテナの価格情報、販売条件（ＵＣＰ）、またはセキュアコンテナのユーザデバイス格納処理の際にユーザデバイスにおいて生成され格納される使用制御情報（ＵＣＳ）のいずれかに格納された個人識別証明書（ＩＤＣ）のリストにユーザのＩＤＣ識別子が格納されることになる。ユーザデバイス１，９２０の格納コンテンツを利用する場合、セキュアコンテナのＩＤＣリストに基づく個人認証処理を実行する。コンテンツ利用を要求するユーザにサンプリング情報の入力を求め、入力されたサンプリング情報と格納された個人識別証明書（ＩＤＣ）内のテンプレートとの照合を実行し、照合が成立した場合にのみ、コンテンツ利用を許可する。

【０２０８】

さらに、セキュアコンテナは、前述の通り、ユーザデバイス間での配信が可能である。セキュアコンテナがユーザデバイス１，９２０から、ユーザデバイス２，９３０に移動された場合、ユーザ９４０，９４５は、ユーザデバイス２，９３０においてコンテンツの利用を行なう場合においても、セキュアコンテナの価格情報、販売条件（ＵＣＰ）、または使用制御情報（ＵＣＳ）のＩＤＣリストに基づく個人認証処理を実行する。コンテンツ利用を要求するユーザにサンプリング情報の入力を求め、入力されたサンプリング情報と格納された個人識別証明書（ＩＤＣ）内のテンプレートとの照合を実行し、照合が成立を条件としてコンテンツ利用を許可する。

【０２０９】

このように、セキュアコンテナの移動があった場合においても、セキュアコンテナに当初格納された価格情報、販売条件（ＵＣＰ）の個人識別証明書（ＩＤＣ）リストは不変であり、またセキュアコンテナの販売条件（ＵＣＰ）に基づいて生成される使用制御情報（ＵＣＳ）のＩＤＣリストも不変であり、これらのＩＤＣリストに基づいてコンテンツの利用者が正当なユーザにのみ制限することが可能となる。

【０２１０】

次に、図４３にセキュアコンテンナを利用したコンテンツのユーザ間の配信処

理、ユーザの個人認証の異なる形態を示す。図４３に示す処理は、ユーザデバイスの使用制限、すなわちアクセス制限をユーザデバイスに格納した個人識別証明書（ＩＤＣ）に基づく個人認証処理により実行し、さらに、コンテンツの使用に際して、セキュアコンテナの価格情報、販売条件（ＵＣＰ）、または使用制御情報（ＵＣＳ）のＩＤＣリストに基づく個人認証処理を実行する２つの認証を実行する形態である。

【０２１１】

ユーザデバイス１，９５０を使用するユーザＡ，ユーザＢは、個人識別認証局（ＩＤＡ）９７０に予めサンプリング情報を提示して、サンプリング情報に基づくテンプレート情報を格納した個人識別証明書（ＩＤＣ）の発行依頼を行なう。発行された個人識別証明書（ＩＤＣ）は、使用するユーザデバイス１，９５０に格納する。

【０２１２】

ユーサデバイス９５０は使用開始にあたり、デバイスに格納された個人識別証明書（ＩＤＣ）９５５に基づく個人認証処理を実行し、使用を要求するユーザにサンプリング情報の入力を求め、入力されたサンプリング情報と格納された個人識別証明書（ＩＤＣ）内のテンプレートとの照合を実行し、照合が成立した場合にのみ、ユーザデバイス１，９５０の使用を許可する。

【０２１３】

さらに、セキュアコンテナ９９０のコンテンツの利用を行なう際には、セキュアコンテナの価格情報、販売条件（ＵＣＰ）、または使用制御情報（ＵＣＳ）のＩＤＣリストに基づく個人認証処理を実行する。ここでユーザに対応するＩＤＣリストが検出されないか、または検出されても入力サンプリング情報と照合が成立しない場合はコンテンツの利用が許可されない。

【０２１４】

すなわち、セキュアコンテナ９９０の格納コンテンツをユーザデバイス１，９５０において利用する際は、ユーザデバイスに格納された個人識別証明書（ＩＤＣ）に基づく個人認証が成立し、さらに、セキュアコンテナの価格情報、販売条件（ＵＣＰ）、または使用制御情報（ＵＣＳ）のＩＤＣリストに基づく個人認証

処理が成立することが要件となる。

【０２１５】

セキュアコンテナは、デバイス間で移動することが可能であり、ユーザデバイス２，９６０に移動した場合は、同様にユーザデバイス２，９６０に格納された個人識別証明書（ＩＤＣ）に基づく個人認証、さらに、セキュアコンテナの価格情報、販売条件（ＵＣＰ）、または使用制御情報（ＵＣＳ）のＩＤＣリストに基づく個人認証処理が実行される。

【０２１６】

図４３の構成では、ユーザデバイス１，９５０にはユーザＡ，Ｂの個人識別証明書（ＩＤＣ）９５５が格納されており、セキュアコンテナにはユーザＡ，Ｂ，Ｃのリスト９９２が格納されているので、ユーザＡ，Ｂのみがユーザデバイス１，９５０を使用してコンテンツの利用が可能となり、ユーザデバイス２，９６０にはユーザＡ，Ｃの個人識別証明書（ＩＤＣ）９６５が格納されており、セキュアコンテナにはユーザＡ，Ｂ，Ｃのリスト９９２が格納されているので、ユーザＡ，Ｃのみがユーザデバイス２，９６０を使用してコンテンツの利用が可能となる。

【０２１７】

なお、図４３の構成例は、各ユーザデバイスにおいては格納ＩＤＣのみとの照合処理を実行することを条件とした認証処理を行なうように設定したシステムである。個人識別証明書（ＩＤＣ）を個人識別認証局（ＩＤＡ）に登録済みのすべてのユーザが使用可能なデバイスとして設定する場合は、デバイスのアクセス権制御をデバイスに格納したＩＤＣのみならず、ＩＤＡに接続してＩＤＡに格納した個人識別証明書（ＩＤＣ）の格納テンプレートと入力サンプリング情報との比較を実行して認証処理を行なうようにしてもよい。

【０２１８】

なお、ユーザデバイス間におけるセキュアコンテナの配信、利用処理においてセキュアコンテナのＩＤＣリストに基づく個人識別証明書（ＩＤＣ）を利用した個人認証を実行してコンテンツの利用制限を実行する処理例を図４４，４５の処理フローに従って説明する。このフローにおいては、ユーザデバイスのアクセス

制限については含まない処理として説明する。

【０２１９】

図４４にセキュアコンテナをユーザデバイスＡから受領し、ユーザデバイスＢにおいて個人認証処理を実行して、正当なユーザにのみコンテンツ利用を可能とした処理フローを示す。以下、フローの各ステップについて説明する。

【０２２０】

ステップＳ７５１では、ユーザデバイスＡとユーザデバイスＢ間で相互認証を実行し、認証成立を条件（Ｓ７５２でＹｅｓ）として、ユーザデバイスＡは、セキュアコンテナを抽出し（Ｓ７５３）、ユーザデバイスＢに送信する（Ｓ７５４）。なお、相互認証時にセッションキーが生成され、以下のユーザデバイス間でのデータ転送は、必要に応じてセッションキーでの暗号化処理が行なわれる。

【０２２１】

ユーザデバイスＢは受信したセキュアコンテナの検証を行なう（Ｓ７５５）、検証には、セキュアコンテナ自体の署名検証、コンテナ内の価格情報、販売条件情報（ＵＣＰ）等の個別データの署名検証処理を含む。

【０２２２】

コンテナ検証が成功すると（Ｓ７５６，Ｙｅｓ）、コンテンツ利用を要求するユーザは、サンプリング情報とユーザＩＤをユーザデバイスＢに入力（Ｓ７５７）し、ユーザデバイスＢは、使用制御情報（ＵＣＳ）から個人識別証明書（ＩＤＣ）リストを抽出し（Ｓ７５８）、ユーザＩＤに基づいて対応するＩＤＣ識別子を検索する（Ｓ７５９）。入力ユーザＩＤに対応するＩＤＣ識別子が検出されない場合は、サービスプロバイダの認めたユーザでないこととなり、エラーとなり（Ｓ７６０でＮｏ）、処理は続行されない。

【０２２３】

個人識別証明書（ＩＤＣ）リストに入力ユーザＩＤに対応するＩＤＣ識別子が検出された場合（Ｓ７６０でＹｅｓ）は、ＩＤＣ識別子に基づいて個人識別証明書（ＩＤＣ）を取得（Ｓ７６１）する。個人識別証明書（ＩＤＣ）は、ユーザデバイスＢに格納されている場合は、ユーザデバイスＢに格納されたＩＤＣを用い、ない場合は、個人識別認証局（ＩＤＡ）、またはサービスプロバイダから取り

寄せる。取得した個人識別証明書（ＩＤＣ）からテンプレートを取り出して、自己の秘密鍵で復号し、テンプレートとサンプリング情報との照合を実行し（Ｓ７６２）、照合が成立しない場合（Ｓ７６３でＮｏ）は、エラーとなり、その後の処理が続行されない。具体的にはコンテンツの復号処理が実行されず、コンテンツの利用が制限される。照合が成立した場合（Ｓ７６３でＹｅｓ）は、照合成立がユーザデバイスＡに通知され、ユーザデバイスＡはセキュアコンテナに格納された暗号化コンテンツの復号に適用するコンテンツ鍵をユーザデバイスＢに送信する（Ｓ７６４）。ユーザデバイスＢでは、ユーザデバイスＡから受信したコンテンツ鍵を使用して暗号化コンテンツの復号を行ないコンテンツを利用（Ｓ７６５）する。

【０２２４】

このように、個人識別証明書（ＩＤＣ）のテンプレートを用いたユーザの個人識別処理を実行し、照合成立により、正当ユーザであることが確認された場合にのみセキュアコンテナに格納されたコンテンツの利用を可能とする構成により、セキュアコンテナがユーザデバイス間で配信された後も、不当なユーザのコンテンツ利用を防止することが可能となる。

【０２２５】

次に、図４５にコンテンツを配信する前に配信元において個人認証処理を実行して、正当なユーザにのみセキュアコンテナを配信する処理フローを示す。以下、フローの各ステップについて説明する。

【０２２６】

ステップＳ７７１では、ユーザデバイスＡとユーザデバイスＢ間で相互認証を実行する。相互認証時にセッションキーが生成され、以下のサービスプロバイダとユーザデバイス間でのデータ転送は、必要に応じてセッションキーでの暗号化処理が行なわれる。

【０２２７】

相互認証成立を条件（Ｓ７７２でＹｅｓ）として、ユーザデバイスＡは、セキュアコンテナを抽出し（Ｓ７７３）、ユーザデバイスＢは、サンプリング情報とユーザＩＤをユーザデバイスに入力（Ｓ７８５）し、これらをユーザデバイスＡ

に送信（Ｓ７８６）する。

【０２２８】

ユーザデバイスＡ、セキュアコンテナの価格情報、販売条件情報（ＵＣＰ）、または使用制御情報（ＵＣＳ）のいずれかから個人識別証明書（ＩＤＣ）リストを抽出し（Ｓ７７４）、ユーザＩＤに基づいて対応するＩＤＣ識別子を検索する（Ｓ７７５）。入力ユーザＩＤに対応するＩＤＣ識別子が検出されない場合は、サービスプロバイダの認めたユーザでないと判定され、エラーとなり（Ｓ７７６でＮｏ）、処理は続行されない。

【０２２９】

個人識別証明書（ＩＤＣ）リストに入力ユーザＩＤに対応するＩＤＣ識別子が検出された場合（Ｓ７７６でＹｅｓ）は、ＩＤＣ識別子に基づいて個人識別証明書（ＩＤＣ）を取得（Ｓ７７７）する。個人識別証明書（ＩＤＣ）は、サービスプロバイダに格納されている場合は、サービスプロバイダに格納されたＩＤＣを用い、ない場合は、個人識別認証局（ＩＤＡ）から取り寄せる。取得した個人識別証明書（ＩＤＣ）からテンプレートを取り出して、自己の秘密鍵で復号し、テンプレートとサンプリング情報との照合を実行し（Ｓ７７８）、照合が成立しない場合（Ｓ７７９でＮｏ）は、エラーとなり、その後の処理が続行されない。具体的にはセキュアコンテナおよびコンテンツ鍵の配信が実行されない。照合が成立した場合（Ｓ７７９でＹｅｓ）は、正当なユーザであると判定され、その後の処理が続行される。具体的にはセキュアコンテナおよびコンテンツ鍵のユーザデバイスＢに対する配信が実行される。

【０２３０】

ユーザデバイスＡがセキュアコンテナをユーザデバイスＢに送信すると、ユーザデバイスＢは受信したセキュアコンテナの検証を行なう（Ｓ７８１）、検証には、セキュアコンテナ自体の署名検証、コンテナ内の価格情報、販売条件情報（ＵＣＰ）等の個別データの署名検証処理を含む。コンテナ検証が成功すると（Ｓ７８２，Ｙｅｓ）、ユーザデバイスＢにおいてセキュアコンテナのコンテンツ利用が可能となる。

【０２３１】

このように、ユーザデバイスＡ側で、個人識別証明書（ＩＤＣ）のテンプレートを用いたユーザの個人識別処理を実行し、照合成立により、正当ユーザであることが確認された場合にのみセキュアコンテナの配信を実行する構成により、不当なユーザに対するコンテンツ配信を防止することが可能となる。

【０２３２】

次に、図４６にユーザデバイス間でのセキュアコンテナの転送処理を実行するユーザデバイス構成を中心としたブロック図を示す。図４６を用いてセキュアコンテナの転送、コンテンツ使用制御情報（ＵＣＳ）生成、格納処理について説明する。

【０２３３】

図４６のサービスプロバイダ１８１０が、セキュアコンテナの最初の流通（一次配布）を行なう。サービスプロバイダ１８１０は、コンテンツデータベース１８１２にコンテンツを格納し、さらに、ユーザ情報データベース１８１３にユーザ情報を格納している。サービスプロバイダ１８１０は、制御部１８１１の制御のもとに暗号処理部１８１４において、セキュアコンテナの転送処理に必要な転送先との相互認証処理、転送データに対する署名処理等を実行する。暗号処理部１８１４は、これら各暗号処理に必要となる鍵情報、さらに、先に説明した公開鍵証明書発行局（ＣＡ）の公開鍵、公開鍵証明書発行局（ＣＡ）の発行した公開鍵証明書等を保持したメモリを有している。また、データベース１８１３にはサービス提供ユーザに関する個人識別証明書（ＩＤＣ）を格納している。必要に応じてＩＤＣを使用して個人識別装置１８１６においてサンプリング情報との照合処理による個人認証を実行する。

【０２３４】

サービスプロバイダ１８１０は、ユーザデバイスＡ１８２０に対してセキュアコンテナを通信部１８１５を介して転送する。セキュアコンテナは先に説明したように、販売条件（ＵＣＰ）、価格情報を含み、少なくともいずれかに個人識別証明書（ＩＤＣ）リストを含む。

【０２３５】

また、図４６に示すクリアリングセンタ１８４０がコンテンツ流通に伴うコン

テン利用料の決済（電子マネー上のデータなど）処理を行なう。クリアリングセンタ１８４０は、通信部１８４５を介して行われる決済用の受領ログ受信または発行ログ送信において各デバイスと認証処理を実行し、また送受信データに対する署名処理、署名検証処理を実行するための暗号処理部１８４４を有し、また、ユーザ管理、ユーザ残高管理用の各種のデータを格納したデータベース１８４２を有する。暗号処理部１８４４には、各暗号処理に必要となる鍵情報、公開鍵証明書発行局（ＣＡ）の公開鍵、公開鍵証明書発行局（ＣＡ）の発行した公開鍵証明書等を保持したメモリを有している。制御部１８４１は、データ送受信、暗号処理部における暗号処理時のデータ転送等の制御を行なう。また、データベース１８４２にはサービス提供ユーザに関する個人識別証明書（ＩＤＣ）を格納している。必要に応じてＩＤＣを使用して個人識別装置１８４６においてサンプリング情報との照合処理による個人認証を実行する。

【０２３６】

サービスプロバイダ１８１０は、ユーザデバイスＡ１８２０に対してセキュアコンテナを通信部１８１５を介して転送して、ユーザデバイスＡ１８２０が通信部１８２７を介してこれを受信し、購入処理を実行する。購入処理においては、記憶部１８２５に格納した個人識別証明書（ＩＤＣ）による個人認証を実行する。なお、個人識別証明書（ＩＤＣ）がない場合は、サービスプロバイダ１８１０において個人認証処理を実行してもよい。ユーザデバイスＡ１８２０は、制御部１８２１の制御のもとに暗号処理部１８２２においてセキュアコンテナの販売条件（ＵＣＰ）等に基づいてコンテンツ使用制限情報（ＵＣＳ）を生成して、これをフラッシュメモリ等のメモリ１８２４に格納する。コンテンツ使用制限情報（ＵＣＳ）には前述したように販売条件（ＵＣＰ）に格納した個人識別証明書（ＩＤＣ）リストを承継したリストを含む。

【０２３７】

ユーザデバイスＡ１８２０は、例えば電子マネー１８２８によるコンテンツ利用料金支払処理を行なう。利用ログを暗号処理部１８２２において生成して、通信部１８２７を介してサービスプロバイダ１８１０に送信する。ユーザデバイスＡ１８２０が受信したセキュアコンテナは、ハードディスク等の記憶部１８２５

に格納される。サービスプロバイダ１８１０は、ユーザデバイスＡ１８２０から送信された利用ログの検証をして、検証が済むと、コンテンツ鍵をセッション鍵で暗号化してユーザデバイスＡ１８２０に送信する。ユーザデバイスＡ１８２０は、暗号化されたコンテンツ鍵をセッション鍵で復号し、これをさらにユーザデバイスＡ１８２０固有の保存鍵で暗号化してメモリ１８２４に格納する。

【０２３８】

ユーザデバイスＡ１８２０は、データ再生部１８２６でのコンテンツ再生等、コンテンツ利用に際しては、メモリ１８２４に保存したコンテンツ鍵を保存鍵で復号して、復号したコンテンツ鍵を用いて記憶部１８２５に格納されたセキュアコンテナ中のコンテンツを復号処理してデータ再生部１８２６において再生する。なお、セキュアコンテナ中のコンテンツの復号処理に際しては、その前ステップとして、メモリ１８２４に格納されたコンテンツ使用制限情報（ＵＣＳ）の再生残り回数等の設定条件を判定し、条件がクリアされた場合には復号が可能となる。

【０２３９】

さらに、セキュアコンテナをユーザデバイスＡ１８２０からユーザデバイスＢ１８３０に配信する場合は、ユーザデバイスＡ１８２０は、メモリ１８２４からコンテンツ使用制限情報（ＵＣＳ）を読み出し、暗号処理部１８２２内で保存鍵で復号化（暗号化されていない場合は復号処理は不要）し、ＵＣＳの「ＵＣＳ世代管理情報」、「ＵＣＳ二次配信可能回数」を判定し、新たな配信が可能と判定された場合には、ユーザデバイスＢ１８３０に対してセキュアコンテナを通信部１８２７を介して転送して、ユーザデバイスＢ１８３０が通信部１８３７を介してこれを受信し、購入処理を実行する。

【０２４０】

なお、セキュアコンテナの配信時には前述の個人認証処理が実行される。個人認証処理は、前述の図４５のフローを用いて説明したようにセキュアコンテナの配信元のユーザデバイスＡの個人識別装置１８２９で実行するか、あるいは図４４のフローを用いて説明したように配信先のユーザデバイスＢの個人識別装置１８３９のいずれかで実行する。また、その他のサービプロバイダ、あるいは個人

識別認証局（ＩＤＡ）において実行するようにしてもよい。

【０２４１】

個人認証が成立すると、ユーザデバイスＢ１８３０は、制御部１８３１の制御のもとに暗号処理部１８３２においてセキュアコンテナの販売条件（ＵＣＰ）とユーザデバイスＡ１８２０のＵＣＳ情報等に基づいて、新たな「ＵＣＳ世代管理情報」、「ＵＣＳ二次配信可能回数」を設定したコンテンツ使用制限情報（ＵＣＳ－Ｂ）を生成して、これをフラッシュメモリ等のメモリ１８３４に格納する。

【０２４２】

この際に生成するＵＣＳ－Ｂは、ユーザデバイスＡ１８２０のコンテンツ利用履歴を継承したものとなる。ＵＣＳ－Ｂの「ＵＣＳ世代管理情報」はＵＣＳ－Ａの「ＵＣＳ世代管理情報」より１つ減じた回数として設定される。ＵＣＳ－Ｂの「ＵＣＳ二次配信可能回数」はＵＣＳ－Ａの「ＵＣＳ二次配信可能回数」より１つ減じた回数として設定する構成と、セキュアコンテナ内の「ＵＣＰ二次配信可能回数」と同一回数を新たに設定する構成とがある。

【０２４３】

ユーザデバイスＢ１８３０は、電子マネー１８３８によるコンテンツ利用料金支払処理、すなわち利用ログを暗号処理部１８３２において生成して、通信部１８３７を介してユーザデバイスＡ１８２０に送信する。ユーザデバイスＢ１８３０が受信したセキュアコンテナは、ハードディスク等の記憶部１８３５に格納される。ユーザデバイスＡ１８２０は、ユーザデバイスＢ１８３０から送信された利用ログの検証をして、検証が済むと、メモリ１８２４からコンテンツ鍵を読み出し、これを保存鍵で復号した後、コンテンツ鍵をセッション鍵で暗号化してユーザデバイスＢ１８３０に送信する。ユーザデバイスＢ１８３０は、暗号化されたコンテンツ鍵をセッション鍵で復号し、これをさらにユーザデバイスＢ１８３０固有の保存鍵で暗号化してメモリ１８３４に格納する。

【０２４４】

また、不正な改竄により設定を超えた使用を行なうと、同一セキュアコンテナに基づいて生成された受領ログ数が、セキュアコンテナ中の販売条件（ＵＣＰ）に含まれる「ＵＣＰ世代管理情報」の設定を超えることとなるため、クリアリン

グセンタ１８４０に送付された場合に無効と判定される。受領ログには、コンテンツＩＤ等の情報とともに、セキュアコンテナに記録された「ＵＣＰ世代管理情報」が記録されており、クリアリングセンタ１８４０における決済処理においては、「ＵＣＰ世代管理情報」の設定を超える受領ログを受信した場合はこれを無効とする。なお、ユーザ間配信の認められない設定のなされたコンテンツに基づいて生成された受領ログについても、その受領ログを無効とする処理を実行する。

【０２４５】

ユーザデバイスＢ１８３０は、データ再生部１８３６でのコンテンツ再生等、コンテンツ利用に際しては、メモリ１８３４に保存したコンテンツ鍵を保存鍵で復号して、復号したコンテンツ鍵を用いて記憶部１８３５に格納されたセキュアコンテナ中のコンテンツを復号処理してデータ再生部１８３６において再生する。なお、セキュアコンテナ中のコンテンツの復号処理に際しては、メモリ１８３４に格納されたコンテンツ使用制限情報（ＵＣＳ）に設定された再生残り回数等の利用可能状況が判定され、設定条件範囲内でコンテンツの利用、すなわち復号が可能となる。

【０２４６】

セキュアコンテナを用いたコンテンツ配信では、サービスプロバイダとユーザデバイス間の一次配布、さらに複数のユーザデバイス間での二次配布（世代間配信または二次配信）において、個人識別証明書（ＩＤＣ）によるユーザ確認が可能となり、また、コンテンツ利用は、セキュアコンテナ中の販売条件（ＵＣＰ）に含まれる「ＵＣＰ世代管理情報」、「ＵＣＰ二次配信可能回数」によって制限された範囲に制限される。また一次配布、二次配布（世代間配信または二次配信）に伴うコンテンツ利用料金回収もセキュアコンテナ中の価格情報、販売条件等に基づいて生成される受領ログに従って自動的に処理可能となるため、決済処理のための新たな処理が不要となる。

【０２４７】

［７．個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）とのリンク］

次に、個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）とを関連付ける構

成、すなわちリンク構成について説明する。

【０２４８】

個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）とは関連付けて管理することが、様々な場面において有効となる。例えば、個人識別証明書（ＩＤＣ）と、該個人識別証明書の格納テンプレートの暗号化に適用した公開鍵の公開鍵証明書とを関連付けるリンクを構成したり、特定のサービスプロバイダ等、データ通信先との接続処理の際の、個人認証、相互認証または暗号処理データ通信を実行する際に適用する個人識別証明書と公開鍵証明書との組合わせについてのリンクを構成することで、一方の証明書に基づいて他方の証明書を特定することが可能となる。

【０２４９】

個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）とのリンクは１対１のリンク、すなわち１つの個人識別証明書（ＩＤＣ）と、１つの公開鍵証明書（ＰＫＣ）とをリンクさせる態様の他に、１対多、多対１、多対多のリンク態様がある。ＰＫＣとＩＤＣの対応が1対1とは、個人識別証明書（ＩＤＣ）によって識別される唯一の個人に唯一の公開鍵証明書（ＰＫＣ）が対応する場合で、例えば使用デバイスと、そのデバイスを使用する個人が１対１に対応する場合である。

【０２５０】

ＰＫＣとＩＤＣの対応が１対Ｎ（Ｎは２以上）とは、複数の個人識別証明書（ＩＤＣ）によって識別される複数の個人と公開鍵証明書が非対応。すなわち、デバイスを複数人で共有する場合等である。ＰＫＣとＩＤＣの対応がＭ対１（Ｍは２以上）とは、個人識別証明書（ＩＤＣ）によって識別される唯一の個人が使用する、または使用できる公開鍵証明書が複数ある場合である。ＰＫＣとＩＤＣの対応がＭ対Ｎ（Ｍ，Ｎは２以上）とは、複数の個人識別証明書（ＩＤＣ）によって識別される複数の個人が使用する、または使用できる公開鍵証明書が複数あり、かつ、デバイスを共有している場合である。

【０２５１】

また、個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）とのリンク態様には、リンク方向、すなわちいずれか一方の証明書から他方の証明書を導くことの

みが可能な一方向リンク（または片方向リンク、有方向リンク）と、いずれの証明書からでも他方の証明書を導くことが可能な双方向リンクとがある。

【０２５２】

図４７，４８に１対１、１対多、多対１、多対多の個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）とのリンク態様のそれぞれについて示す。いずれの場合も個人識別証明書（ＩＤＣ）は、個人識別認証局（ＩＤＡ）によって発行され個人識別認証局（ＩＤＡ）の署名が付加された証明書であり、公開鍵証明書（ＰＫＣ）は認証局（ＣＡ）によって発行され、認証局（ＣＡ）の署名が付加されている。

【０２５３】

リンクの実現方法としては、いずれの場合においても、以下に示す各種の実現方法がある。

①ＰＫＣ識別番号をＩＤＣに埋め込む。

（ＩＤＣからＰＫＣへの１方向リンク）

②ＩＤＣ識別番号をＰＫＣに埋め込む。

（ＰＫＣからＩＤＣへの１方向リンク）

③リンク構造体ＩＤをＩＤＣ、ＰＫＣに埋め込む。リンク構造体はリンク構造体ＩＤによって識別され、リンク関係のＩＤＣ識別番号、ＰＫＣ識別番号を持つ。

（ＩＤＣ、ＰＫＣの双方向リンク）

④ ＰＫＣ識別番号とＩＤＣ識別番号の組を証明書外に記録する。

（ＩＤＣからＰＫＣへの１方向リンク）

⑤ ＰＫＣ識別番号とＩＤＣ識別番号の組を証明書外に記録する。

（ＰＫＣからＩＤＣへの１方向リンク）

⑥ ＰＫＣ識別番号とＩＤＣ識別番号の組を証明書外に記録する。

（ＩＤＣ、ＰＫＣの双方向リンク）

⑦ＩＤＣ内にＰＫＣを格納する。

（ＩＤＣからＰＫＣへの１方向リンク）

⑧ＰＫＣ内にＩＤＣを格納する。

（ＰＫＣからＩＤＣへの１方向リンク）

⑨各証明書内にリンク情報問い合わせ番号、問い合わせ情報を格納する。

（ＰＫＣ、ＩＤＣのいずれか１方向、または双方向リンク）

【０２５４】

上述のように、リンク情報の格納態様としては、①、②に示すように、個人識別証明書（ＩＤＣ）または公開鍵証明書（ＰＫＣ）自身の内部に、リンク証明書の識別番号を格納（埋め込む）する方法、③に示すように、リンク関係にある各証明書の識別番号の対応を示すリンク構造体を生成してそのリンク構造体の識別子（ＩＤ）を関連付けた個人識別証明書（ＩＤＣ）または公開鍵証明書（ＰＫＣ）に記録する方法、すなわち、リンク識別データとしてのリンク構造体識別子と、リンクを構成する公開鍵証明書識別子と、個人識別証明書識別子とをデータとして格納する構成、さらに、④、⑤、⑥に示すように、それぞれの証明書とは、異なる外部、例えばネットワーク上に配置したリンク情報管理センター等の機関において、個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）とのリンク情報を集積して管理し、必要に応じてリンク情報を抽出可能にする構成等がある。各リンク態様の具体的構成について、説明する。

【０２５５】

（ＩＤＣ内にＰＫＣを格納）

前述したように個人識別のためのテンプレート情報の個人識別証明書（ＩＤＣ）における格納態様の一態様には、公開鍵でテンプレートを暗号化して格納する構成がある。このテンプレートを暗号化した公開鍵に対応して生成された公開鍵証明書（ＰＫＣ）が、個人識別証明書（ＩＤＣ）のリンク公開鍵証明書（ＰＫＣ）として設定され、このリンク公開鍵証明書（ＰＫＣ）を個人識別証明書（ＩＤＣ）に格納する。図４９（ａ）にリンク公開鍵証明書（ＰＫＣ）の個人識別証明書（ＩＤＣ）に対する格納態様を説明する図を示す。

【０２５６】

図４９（ａ）に示すように、個人識別証明書（ＩＤＣ）には、暗号化されたテンプレート、およびそのテンプレート暗号化に適用した公開鍵に対応する公開鍵証明書（ＰＫＣ）が格納される。なお、テンプレート暗号化に適用する公開鍵は、前述のように、ユーザまたはユーザデバイスの公開鍵、サービスプロバイダ（

ＳＰ）の公開鍵、または、個人識別認証局（ＩＤＡ）の公開鍵のいずれかであり、格納される公開鍵証明書（ＰＫＣ）は、そのテンプレート暗号化に適用した公開鍵の公開鍵証明書（ＰＫＣ）である。このようなリンク構成を採用することにより、個人識別証明書（ＩＤＣ）と、テンプレート（Template）を暗号化した公開鍵の公開鍵証明書（ＰＫＣ）が強く結びつき、２種類の証明書が不可分になる。ただし、このリンク構成を採用する場合は、ＩＤＣ有効期限年月日＜＝ＰＫＣ有効期限年月日として設定する。すなわち、ＩＤＣに格納されるＰＫＣはＩＤＣの有効期限において常に有効である設定とすることが好ましい。

【０２５７】

（ＰＫＣ内にＩＤＣを格納）

また、テンプレートを暗号化した公開鍵に対応して生成された公開鍵証明書（ＰＫＣ）の内部に、公開鍵証明書（ＰＫＣ）のリンク個人識別証明書（ＩＤＣ）を格納した構成例を図４９（ｂ）に示す。

【０２５８】

図４９（ｂ）に示すように、公開鍵証明書（ＰＫＣ）には、その公開鍵証明書（ＰＫＣ）に対応する公開鍵を適用して暗号化されたテンプレート情報を持つ個人識別証明書（ＩＤＣ）が格納される。なお、テンプレート暗号化に適用する公開鍵は、前述のように、ユーザまたはユーザデバイスの公開鍵、サービスプロバイダ（ＳＰ）の公開鍵、または、個人識別認証局（ＩＤＡ）の公開鍵のいずれかであり、個人識別証明書（ＩＤＣ）を格納した公開鍵証明書（ＰＫＣ）は、そのテンプレート暗号化に適用した公開鍵の公開鍵証明書（ＰＫＣ）である。このようなリンク構成を採用することにより、個人識別証明書（ＩＤＣ）と、テンプレート（Template）を暗号化した公開鍵の公開鍵証明書（ＰＫＣ）が強く結びつき、２種類の証明書が不可分になる。なお、個人識別証明書（ＩＤＣ）自体は独立に存在する。また、このリンク構成を採用する場合は、ＰＫＣ有効期限年月日＜＝ＩＤＣ有効期限年月日として設定する。すなわち、ＰＫＣに格納されるＩＤＣはＰＫＣの有効期限において常に有効である設定とすることが好ましい。

【０２５９】

（リンク証明書の識別子を証明書に格納）

次にリンクする証明書の識別子、例えば各証明書に対応して設定された固有の識別番号を被リンク証明書内のデータとして格納する態様について説明する。

【０２６０】

図５０（ａ）に公開鍵証明書（ＰＫＣ）の識別番号を個人識別証明書（ＩＤＣ）に格納する構成例、図５０（ｂ）に個人識別証明書（ＩＤＣ）の識別番号を公開鍵証明書（ＰＫＣ）に格納する構成例を示す。

【０２６１】

図５０（ａ）に示す公開鍵証明書（ＰＫＣ）の識別番号を個人識別証明書（ＩＤＣ）に格納する場合の公開鍵証明書（ＰＫＣ）は、前述の例と同様、個人識別証明書（ＩＤＣ）に格納されたテンプレートの暗号化に適用した公開鍵に対応する公開鍵証明書（ＰＫＣ）である。この場合、個人識別証明書（ＩＤＣ）の発行以前に公開鍵証明書（ＰＫＣ）が発行済みであることが条件となる。また、有効期限の切れた公開鍵証明書（ＰＫＣ）のリンク情報を格納しても無意味であるので、ＩＤＣ有効期限年月日＜＝ＰＫＣ有効期限年月日として設定された関係であることが好ましい。この構成は、ＰＫＣをＩＤＣ内部に格納する必要がない場合、ＰＫＣをＩＤＣに伴って配布することが好ましくない場合等に利用される。

【０２６２】

また、図５０（ｂ）に示す個人識別証明書（ＩＤＣ）の識別番号を公開鍵証明書（ＰＫＣ）に格納する場合は、個人識別証明書（ＩＤＣ）に格納されたテンプレートの暗号化に適用した公開鍵に対応する公開鍵証明書（ＰＫＣ）のみならず、個人識別証明書（ＩＤＣ）に何らかの関連を持つ公開鍵証明書（ＰＫＣ）の識別子を格納することが可能である。１つの個人識別証明書（ＩＤＣ）に複数の個人識別証明書（ＩＤＣ）を関係づけることが可能である。ＩＤＣの有効期限年月日とＰＫＣの有効期限年月日の大小関係は、それぞれの証明書の有効性に影響を受けない。ただし、ＩＤＣのテンプレートを暗号化するために使用した公開鍵の証明書だけは、その有効期限がＩＤＣ＜＝ＰＫＣでなくてはならない。

【０２６３】

この構成の使用例としては、個人識別証明書（ＩＤＣ）を使って機器のアクセスに対して個人認証を行った後、サービス毎に公開鍵ペアが必要となる場合、複

数のリンク公開鍵証明書（ＰＫＣ）を利用する場合がある。

【０２６４】

（ＰＫＣ，ＩＤＣの組情報を別管理）

次に、個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）との組情報（リンク情報）をＩＤＣ，ＰＫＣとは別のリンク管理用データとして保持し、ＩＤＣ，ＰＫＣ内には、リンク管理用データにアクセス可能な情報を格納した形態について説明する。

【０２６５】

図５１、図５２にリンク管理用データを用いた管理構成例を示す。図５１（ａ）は、個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）との識別子（番号）と、それぞれの有効期限を格納した組情報（リンク情報）を関係データとして保持した構成である。本構成の特徴は、各証明書の登録・発行タイミングを独立とすることができること。証明書関係の記録を必要な場所で生成し管理することで他に影響を与えることがないことがある。関係データの有効期限は、リンク関係のある各証明書の有効期限中、最も短い期限内に設定することが好ましい。一つのＩＤＣで複数のサービスにおける個人認証を行う場合で、各サービス毎に異なる公開鍵ペアを使用する必要がある場合等のリンク管理に有効な形態である。

【０２６６】

図５１（ｂ）は、個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）との識別子（番号）と、それぞれの有効期限を格納した組情報（リンク情報）を関係データとして保持するとともに、組情報を識別するための識別子としての組情報シリアル番号を各証明書に格納した構成である。組情報のシリアル番号は、組情報の管理主体が割り当てる組情報固有の識別データである。リンク関係を持つＰＫＣ，ＩＤＣの発行に際しては、組情報のシリアル番号データを内部データとして格納する。本構成の特徴は、組情報データの関連情報の追加・変更・削除操作が可能であり、これらの操作が証明書自体に影響を与えないことである。本構成は、例えば、サービスプロバイダにおいてＩＤＣとＰＫＣ、およびサービス関連情報を管理する要請の下、サービス提供対象のＩＤＣ、ＰＫＣ情報を組情報を用いて管理する形態において有効な構成である。

【０２６７】

図５２（ｃ）は、個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）に、組情報を識別するための識別子としての組情報シリアル番号を格納し、この組情報を一次情報として定義し、さらに、関連情報を二次情報として、一次情報からアクセス可能な構成としたものである。必要に応じて二次情報から一次情報に対するアクセスも可能な構成とする。一次情報に関連する二次情報は、複数、分散して管理することが可能であり、シリアル番号はＰＫＣ、ＩＤＣの必要な証明書に保存するよう登録発行依頼を行う。関連情報の追加・変更・削除操作は証明書自体に影響を与えない。

【０２６８】

図５２（ｄ）は、個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）との識別子（番号）を格納した組情報（リンク情報）を関係データとして保持するとともに、この組情報を一次情報として定義し、さらに、関連情報を二次情報として、一次情報からアクセス可能な構成としたものである。必要に応じて二次情報から一次情報に対するアクセスも可能な構成とする。

【０２６９】

関連情報を複数の場所に分散して管理する場合は、一次情報に二次情報識別データとインデックス情報を収めておくことで、情報の管理運用が柔軟にできる。例えば様々なサービスプロバイダ（ＳＰ）が一次情報、または二次情報いずれかの管理主体となり、各ＳＰは、それぞれの管理情報を顧客情報として、サービス提供対象となるユーザの個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）のアクセスが可能となる。

【０２７０】

上述のように、様々な態様で、個人識別証明書（ＩＤＣ）と、該個人識別証明書の格納テンプレートの暗号化に適用した公開鍵の公開鍵証明書とを関連付けるリンクを構成したり、特定のサービスプロバイダ等データ通信先との接続処理の際の、個人認証、相互認証または暗号処理データ通信を実行する際に適用する個人識別との接続処理の際に適用する個人識別証明書と公開鍵証明書との組合わせについてのリンクを構成することで、一方の証明書から他方の証明書を導くこと

が容易となり、例えばテンプレートの暗号化、復号処理に適用する鍵を特定する処理や、サービスプロバイダに対する個人識別証明書を利用した個人認証の後に、公開鍵証明書を利用した相互認証を行なう場合等に、必要なデータを迅速に特定することが可能となる。

【０２７１】

［８．個人識別証明書（ＩＤＣ）による認証と公開鍵証明書（ＰＫＣ）に基づくコンテンツ利用処理］

次に、個人識別証明書（ＩＤＣ）による個人認証を行ない、音楽データ、画像データ等のコンテンツをサービスプロバイダが受信（ダウンロード）する処理について、具体的に説明する。

【０２７２】

これまでの説明から明らかなように、個人識別証明書による個人認証のためには、サンプリング情報とテンプレートの比較照合を実行し、その結果を出力するシステムが必要となる。ここでは、ユーザの使用するコンテンツ再生機器としてのユーザデバイスにサンプリング情報とテンプレートの比較照合処理を実行する機構を備え、照合結果に応じてサービスプロバイダに対するネットワークを介したコンテンツのダウンロード処理、あるいはサービスプロバイタに対するユーザ登録処理、契約処理、ユーザ登録抹消処理、さらに個人識別認証局（ＩＤＡ）に対する個人識別証明書（ＩＤＣ）の発行要求処理を実行するシステム構成、および処理方法について説明する。

【０２７３】

図５３に個人認証を実行し、かつコンテンツ再生可能なユーザデバイスの構成を示す。ユーザデバイス５００は、コンテンツ再生機構部５０１、コンテンツデータ蓄積部５０２、個人識別装置５０３、ネットワーク接続部５０４、公開鍵暗号処理部５０５、選択機能部５０６、入出力機能部５０７を有する。

【０２７４】

コンテンツ再生機構部５０１は、コンテンツデータ蓄積部にあるデータを読み出し、再生する機能をもつ。コンテンツデータ蓄積部５０２は、コンテンツデータをネットワークを通じてダウンロードし、蓄える機能をもつ。個人識別装置５

０３は、利用者から個人を識別するために必要な情報としてのサンプリング情報を入力し、デジタルデータに変換する機能と、変換したデジタルデータと、既登録デジタルデータであるテンプレートとの比較照合を実行する機能をもつ。ネットワーク接続部５０４は、ユーザデバイスとネットワークを接続する機能をもつ。公開鍵暗号処理部５０５は、指定されたデータに対して署名をつける機能と、指定された暗号データを復号する機能と、指定されたデータを暗号化する機能と、公開鍵と秘密鍵のペアを作成する機能と、任意の公開鍵証明書とあるデータのリンクを作る機能をもつ。公開鍵暗号処理部５０５はＳＡＭ（Secure Application Module）として構成されている。選択機能部５０６は、再生時にデータを選択する機能と、ネットワークに接続する時、接続先を選択する機能と、ダウンロード時にコンテンツのタイトルを選択する機能をもつ。入出力機能部５０７は、ユーザインターフェースを実現する。表示デバイスや入力デバイスをコントロールし、指定された情報を表示したり、利用者から入力された情報を処理可能なデータに変換する。

【０２７５】

ここで、ユーザデバイス５００の公開鍵暗号処理部５０５には、公開鍵証明書（ＰＫＣ）、個人識別証明書（ＩＤＣ）が格納されており、これらは相互にリンクされたデータ形式、すなわち、いずれかの証明書から他方の証明書を特定することが可能なデータを有する構成である。具体的なリンク形態については、前述の［個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）とのリンク］の項目を参照されたい。ユーザは、公開鍵暗号処理部５０５に格納された個人識別証明書（ＩＤＣ）により、個人認証を実行し、サービスプロバイダとの取り引きにおいて公開鍵証明書（ＰＫＣ）を使用する。

【０２７６】

（コンテンツダウンロード処理）

上述の構成を持つユーザデバイスにおいて、サンプリング情報とテンプレートの比較照合処理の結果に基づいて、サービスプロバイダから音楽データ、画像データ等のコンテンツのダウンロードおよび再生を行なう処理について説明する。図５４にコンテンツダウンロード処理におけるデータの流れを説明する図を示し

、詳細処理フローを図５５，図５６，図５７に示す。以下、これらの図を参照して処理を説明する。なお、以下の説明では、図５４の番号を（ｎ）、図５５～５７のステップ番号（Ｓｎｎｎ）として示す。

【０２７７】

まず、（１）デバイスを使うために、利用者は個人の指紋情報等のサンプリングデータをデバイスに入力する（Ｓ３０１）。（２）個人識別装置は、入力されたサンプリングデータと、既に格納している個人識別証明書（ＩＤＣ）内のテンプレートを比較するために、ＳＡＭに対して個人識別証明書（ＩＤＣ）を要求する（Ｓ３０２）。

【０２７８】

次に、（３）リンク情報を使い、個人識別証明書（ＩＤＣ）を検索し、ＩＤＣまたはＩＤＣから抽出したテンプレートを個人識別装置に渡す（Ｓ３０３～Ｓ３０５）。（４）個人識別装置は、サンプリングデータとテンプレートの照合処理（Ｓ３０６）を実行し、照合成立と判定し、個人認証成立と認められる利用者であると判断した場合、利用者とネットワーク接続部に対して個人認証成功を通知する（Ｓ３０７，Ｓ３０８）。この個人認証成立を条件として、ネットワーク接続部はネットワーク接続のための準備を行う（Ｓ３０９）。

【０２７９】

（５）利用者は入出力機能部が提供するインターフェースを利用して、再生したいデータを指示・操作する（Ｓ３１０，Ｓ３１１）。（６）選択機能部は、インターフェースを通して受け付けた指示を変換し、ネットワーク接続部への制御指示を生成（Ｓ３１１，Ｓ３１２）し、制御指示をネットワーク接続部へ渡す（Ｓ３１３）。

【０２８０】

次に、（７）ネットワーク接続部は、必要なコンテンツデータの取り引きにおいて必要となる公開鍵証明書（ＰＫＣ）を公開鍵暗号処理部に要求する（Ｓ３１４～Ｓ３１６）。（８）公開鍵暗号処理部は、要求された公開鍵証明書（ＰＫＣ）をネットワーク接続部に渡す（Ｓ３１７）。なお、必要に応じて、公開鍵暗号処理部はＩＤＣとＰＫＣのリンクをたどり必要なＰＫＣを探して、見つけたＰＫ

Ｃをネットワーク接続部に渡す処理を実行する。

【０２８１】

次に、（９）ネットワーク接続部は、ローカルネットワークやインターネットを介して、コンテンツデータ提供サーバにアクセスする（Ｓ３１８）。デバイスとサーバとの間で公開鍵証明書ベースの相互認証を行い、セッション鍵を共有するなどして、秘匿通信路を確保する（Ｓ３１９）。図５４に示す（９－１）～（９－８）は、サービス利用に関して、インタラクティブに利用者とサーバが情報交換を行う必要がある場合の処理で、必要な回数繰り返す（Ｓ３２０，Ｓ３２１）。コンテンツ提供サーバからのデータが（９－１）～（９－４）を介して利用者に送信され、ユーザからの送信データが（９－５）～（９－８）でコンテンツ提供サーバーに流れる。このデータ送受信においては、必要に応じてセッションキーによる暗号化処理、それぞれの秘密鍵による署名処理、公開鍵による署名検証処理等のデータ検証処理を行なうことが好ましい。

【０２８２】

一連のデータのやり取りが終了すると、（１０）ネットワーク接続部は、コンテンツ提供サーバから必要なコンテンツデータをダウンロードする（Ｓ３２２）。次に、（１１）ネットワーク接続部は、ダウンロードしたコンテンツデータをコンテンツデータ蓄積部に渡しコンテンツデータを保存し、（Ｓ３２３）セッションを終了する（Ｓ３２４）。

【０２８３】

次に、（１２）データ再生が利用者から要求されていた場合は、コンテンツデータをコンテンツ再生機構部に渡す（Ｓ３２５でＹｅｓ）。（１３）利用者は、コンテンツ再生機構部でコンテンツの再生を実行（Ｓ３２６）し、入出力機能部を介して利用する。

【０２８４】

以上が、コンテンツのダウンロード、再生処理の流れである。ただし、上述した処理は、コンテンツのダウンロード時に公開鍵証明書（ＰＫＣ）、個人識別証明書（ＩＤＣ）の利用を行ない、かつその２つの証明書がＳＡＭ内部に格納されている順調な処理の流れである。図５５～５７の処理フローには、証明書がない

場合、必要としない場合の処理についても示している。これらの処理について説明する。

【０２８５】

図５６のステップＳ３２８～Ｓ３３２の処理は、ユーザデバイス内に対応する個人識別証明書（ＩＤＣ）が検出されない場合の処理である。この場合、ユーザデバイスは、入出力機能部を介してＩＤＣが見つからない旨のメッセージを表示し（Ｓ３２８）、ＩＤＣの発行要求を実行するか否かをユーザに判断させ（Ｓ３２９）、ユーザからの入力により発行要求を行なわないとされた場合は、ダウンロード失敗を利用者に通知する（Ｓ３３２）。一方、利用者からの入力によりＩＤＣ発行要求を行なうとの意思表示がなされた場合は、コンテンツのダウンロード処理を終了し、ＩＤＣ発行要求処理に移行することを入出力機能部を介して通知する（Ｓ３３０）。その後、ＩＤＣの発行処理を実行する（Ｓ３３１）。この処理の詳細は、前述の［テンプレート、個人識別証明書（ＩＤＣ）の登録、変更処理］の欄を参照されたい。

【０２８６】

図５７のステップＳ３３３以下は、公開鍵証明書（ＰＫＣ）がユーザデバイスに保存されていない場合の処理を示している。公開鍵証明書（ＰＫＣ）を外部機関である認証局（ＣＡ）から取得して受信することを望む場合（Ｓ３３３）、既に登録済みの公開鍵証明書（ＰＫＣ）の有無を判定（Ｓ３３４）し、ある場合は、その公開鍵証明書（ＰＫＣ）を認証局（ＣＡ）から取得してユーザデバイスに格納する（Ｓ３３５）。

【０２８７】

登録済みの公開鍵証明書（ＰＫＣ）が無い場合は、新規発行処理となり、公開鍵、秘密鍵の鍵ペアを生成して、公開鍵証明書（ＰＫＣ）の発行機関であるＲＡ（登録局）に対して新規発行要求を行なう（Ｓ３３６）。新規に公開鍵証明書（ＰＫＣ）が発行された場合は、個人識別証明書（ＩＤＣ）とのリンク情報としての組情報を生成して、公開鍵証明書を格納する（Ｓ３３８）。ただし、前述したようにリンク情報の保有形態には、様々な形態があるので、各証明書内部にリンクデータを格納している証明書構成であれば、必ずしも組情報を生成して保存す

る処理は必要とされない。

【０２８８】

Ｓ３３９以下は、新規の公開鍵証明書（ＰＫＣ）の発行が拒否された場合の処理であり、この場合、ユーザデバイスは、入出力機能部を介してダウンロード失敗を通知して処理を終了する。

【０２８９】

（ユーザ登録、抹消、サービス契約処理）

次に、コンテンツの提供、商品販売、決済処理等の様々なサービスを提供するサービスプロバイダに対しての、ユーザ登録、ユーザ登録抹消、サービス契約処理等を図５３に示すユーザデバイス、すなわちテンプレートとサンプリング情報との比較照合処理を実行する個人識別装置を有する構成での照合処理に基づいて実行する構成について説明する。図５８にユーザ登録、ユーザ登録抹消、サービス契約処理におけるデータの流れを説明する図を示し、詳細処理フローを図５９、図６０、図６１に示す。以下、これらの図を参照して処理を説明する。なお、以下の説明では、図５８の番号を（ｎ）、図５９～６１のステップ番号（Ｓｎｎｎ）として示す。

【０２９０】

まず、（１）デバイスを使うために、利用者は個人の指紋情報等のサンプリングデータをデバイスに入力する（Ｓ４０１）。（２）個人識別装置は、入力されたサンプリングデータと、既に格納している個人識別証明書（ＩＤＣ）内のテンプレートを比較するために、ＳＡＭに対して個人識別証明書（ＩＤＣ）を要求する（Ｓ４０２）。

【０２９１】

次に、（３）リンク情報を使い、個人識別証明書（ＩＤＣ）を検索し、ＩＤＣまたはＩＤＣから抽出したテンプレートを個人識別装置に渡す（Ｓ４０３～Ｓ４０５）。（４）個人識別装置は、サンプリングデータとテンプレートの照合処理（Ｓ４０６）を実行し、照合成立と判定し、個人認証成立と認められる利用者であると判断した場合、利用者とネットワーク接続部に対して個人認証成功を通知する（Ｓ４０７，Ｓ４０８）。この個人認証成立を条件として、ネットワーク接

続部はネットワーク接続のための準備を行う（Ｓ４０９）。

【０２９２】

（５）利用者は入出力機能部が提供するインターフェースを利用して、処理に対応したデータ入力、すなわちユーザ登録であれば、希望登録サイト、ユーサ登録抹消であれば、抹消を希望するサイト、契約処理であれば契約を希望するサイト等のデータ入力を実行する（Ｓ４１０）。（６）選択機能部は、インターフェースを通して受け付けた指示を変換し、ネットワーク接続部への制御指示を生成し、制御指示をネットワーク接続部へ渡す（Ｓ４１１）。

【０２９３】

次に、（７）ネットワーク接続部は、必要なコンテンツデータの取り引きにおいて必要となる公開鍵証明書（ＰＫＣ）を公開鍵暗号処理部に要求する（Ｓ４１２）。（８）公開鍵暗号処理部は、要求された公開鍵証明書（ＰＫＣ）をネットワーク接続部に渡す（Ｓ４１３～Ｓ４１５）。なお、必要に応じて、公開鍵暗号処理部はＩＤＣとＰＫＣのリンクをたどり必要なＰＫＣを探して、見つけたＰＫＣをネットワーク接続部に渡す処理を実行する。

【０２９４】

次に、（９）ネットワーク接続部は、ローカルネットワークやインターネットを介して、サービス登録サーバまたはユーザ登録サーバにアクセスする（Ｓ４１６）。デバイスとサーバとの間で公開鍵証明書ベースの相互認証を行い、セッション鍵を共有するなどして、秘匿通信路を確保する（Ｓ４１７）。図５８に示す（９－１）～（９－８）は、サービス利用に関して、インタラクティブに利用者とサーバが情報交換を行う必要がある場合の処理で、必要な回数繰り返す（Ｓ４１８，Ｓ４１９）。サービス登録サーバまたはユーザ登録サーバからのデータが（９－１）～（９－４）を介して利用者に送信され、ユーザからの送信データが（９－５）～（９－８）でサービス登録サーバまたはユーザ登録サーバに流れる。このデータ送受信においては、必要に応じてセッションキーによる暗号化処理、それぞれの秘密鍵による署名処理、公開鍵による署名検証処理等のデータ検証処理を行なうことが好ましい。

【０２９５】

一連のデータのやり取りが終了すると、（１０）ネットワーク接続部は、サービス登録サーバまたはユーザ登録サーバから必要なデータをダウンロードする（Ｓ４２０）。次に、（１１）ネットワーク接続部は、処理（ユーザ登録、ユーザ登録抹消、契約処理等）が成功した場合に、公開鍵暗号処理部に処理成功を通知する。さらに、必要であれば、個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）とのリンク情報（組情報）に必要な情報を追加する（Ｓ４２２，４２３）。前述したようにリンク情報の保有形態には、様々な形態があるので、各証明書内部にリンクデータを格納している証明書構成であれば、必ずしも組情報を生成して保存する処理は必要とされない。（１２）これらの処理が終了すると、処理結果を入出力機能部を介して表示して処理を終了する（Ｓ４２４，Ｓ４２５）。

【０２９６】

以上が、ユーザ登録、ユーザ登録抹消、サービス契約等、サービスプロバイダとの対応において、個人識別証明書（ＩＤＣ）を適用して個人認証処理を実行する場合の処理の流れである。ただし、上述した処理は公開鍵証明書（ＰＫＣ）、個人識別証明書（ＩＤＣ）の利用を行ない、かつその２つの証明書がＳＡＭ内部に格納されている順調な処理の流れである。図６０～６２の処理フローには、証明書がない場合、必要としない場合の処理についても示している。これらの処理について説明する。

【０２９７】

図６０のステップＳ４２６～Ｓ４３０の処理は、ユーザデバイス内に対応する個人識別証明書（ＩＤＣ）が検出されない場合の処理である。この場合、ユーザデバイスは、入出力機能部を介してＩＤＣが見つからない旨のメッセージを表示し（Ｓ４２６）、ＩＤＣの発行要求を実行するか否かをユーザに判断させ（Ｓ４２７）、ユーザからの入力により発行要求を行なわないとされた場合は、処理失敗を利用者に通知する（Ｓ４３０）。一方、利用者からの入力によりＩＤＣ発行要求を行なうとの意思表示がなされた場合は、コンテンツのダウンロード処理を終了し、ＩＤＣ発行要求処理に移行することを入出力機能部を介して通知する（Ｓ４２８）。その後、ＩＤＣの発行処理を実行する（Ｓ４２９）。この処理の詳細は、前述の［テンプレート、個人識別証明書（ＩＤＣ）の登録、変更処理］の

欄を参照されたい。

【０２９８】

図６１のステップＳ４３１以下は、公開鍵証明書（ＰＫＣ）がユーザデバイスに保存されていない場合の処理を示している。公開鍵証明書（ＰＫＣ）を外部機関である認証局（ＣＡ）から取得して受信することを望む場合（Ｓ４３１）、既に登録済みの公開鍵証明書（ＰＫＣ）の有無を判定（Ｓ４３２）し、ある場合は、その公開鍵証明書（ＰＫＣ）を認証局（ＣＡ）から取得してユーザデバイスに格納する（Ｓ４３３）。

【０２９９】

登録済みの公開鍵証明書（ＰＫＣ）が無い場合は、新規発行処理となり、公開鍵、秘密鍵の鍵ペアを生成して、公開鍵証明書（ＰＫＣ）の発行機関であるＲＡ（登録局）に対して新規発行要求を行なう（Ｓ４３４）。新規に公開鍵証明書（ＰＫＣ）が発行された場合は、個人識別証明書（ＩＤＣ）とのリンク情報としての組情報を生成して、公開鍵証明書を格納する（Ｓ４３６）。ただし、前述したようにリンク情報の保有形態には、様々な形態があるので、各証明書内部にリンクデータを格納している証明書構成であれば、必ずしも組情報を生成して保存する処理は必要とされない。

【０３００】

ステップＳ４３７、Ｓ４３８は、ユーザ登録、ユーザ登録抹消、サービス契約等の各種処理が拒否された場合の処理であり、この場合、ユーザデバイスは、入出力機能部を介して処理失敗を通知して処理を終了する。また、ステップＳ４３９，Ｓ４４０は、新規の公開鍵証明書（ＰＫＣ）の発行が拒否された場合の処理であり、この場合、ユーザデバイスは、入出力機能部を介して処理失敗を通知して処理を終了する。

【０３０１】

（デバイスに格納する個人識別証明書（ＩＤＣ）の要求、登録処理）

次に、図５３に示すような個人識別装置を有するユーザデバイスに格納する個人識別証明書（ＩＤＣ）の発行、登録処理手続きについて説明する。図６２にデバイスに格納する個人識別証明書（ＩＤＣ）の要求処理におけるデータの流れを

説明する図を示し、詳細処理フローを図６３、図６４、図６５に示す。以下、これらの図を参照して処理を説明する。なお、以下の説明では、図６２の番号を（ｎ）、図６３～６５のステップ番号（Ｓｎｎｎ）として示す。

【０３０２】

まず、（１）デバイスを使うために、利用者は個人の指紋情報等のサンプリングデータをデバイスに入力する（Ｓ５０１）。（２）個人識別装置は、入力されたサンプリングデータと、既に格納している個人識別証明書（ＩＤＣ）内のテンプレートを比較するために、ＳＡＭに対して個人識別証明書（ＩＤＣ）を要求する（Ｓ５０２）。なお、ここでは、ユーザデバイスに発行済みの個人識別証明書（ＩＤＣ）がｎ個存在し、さらに新たなテンプレートを格納した個人識別証明書（ＩＤＣ）の発行を要求する処理を行なうものとする。デバイスに個人識別証明書（ＩＤＣ）が全く存在しない場合は、ｎ＝０とした処理となる。

【０３０３】

ユーザデバイスは、（３）格納済みのｎ個の個人識別証明書（ＩＤＣ）を、順次検索し、ＩＤＣまたはＩＤＣから抽出したテンプレートを個人識別装置に渡す（Ｓ５０３～Ｓ５０５）。（４）個人識別装置は、サンプリングデータとテンプレートの照合処理（Ｓ５０６）を実行し、照合成立と判定し、個人認証成立と認められる利用者であると判断した場合、利用者に対して個人認証成功を通知する（Ｓ５０７，Ｓ５０８）。ただし、ここでの処理は、新たなテンプレートを持つ個人識別証明書（ＩＤＣ）の発行を要求するものであり、サンプリングデータと一致する個人識別証明書（ＩＤＣ）は格納されていないとする。すべての格納ＩＤＣと照合しても一致するテンプレートを格納したＩＤＣが見つからない場合、ステップＳ５０９に進む。

【０３０４】

ユーザデバイス内にサンプリング情報と一致するテンプレートを持つ個人識別証明書（ＩＤＣ）が検出されない場合、ユーザデバイスは、入出力機能部を介してＩＤＣが見つからない旨のメッセージを表示（Ｓ５０９）し、ＩＤＣの発行要求を実行するか否かをユーザに判断させ（Ｓ５１０）、ユーザからの入力により発行要求を行なわないとされた場合は、処理終了を利用者に通知する（Ｓ５１２

）。一方、利用者からの入力によりＩＤＣ発行要求を行なうとの意思表示がなされた場合は、ＩＤＣ発行要求処理に移行することを入出力機能部を介して通知する（Ｓ５１１）。

【０３０５】

図６４に示すステップＳ５１３以下の処理は、個人識別証明書（ＩＤＣ）の発行処理において使用する公開鍵証明書（ＰＫＣ）の発行処理フローである。

【０３０６】

ステップＳ５１３では、個人識別証明書（ＩＤＣ）の発行処理に公開鍵証明書（ＰＫＣ）が必要か否かを判定し、必要である場合いは、ステップＳ５１４で、ユーザデバイスの公開鍵暗号処理部に格納されたＩＤＣ、ＰＫＣまたはリンク（組）情報から公開鍵証明書（ＰＫＣ）の識別番号を取得する。公開鍵証明書（ＰＫＣ）が存在した場合（Ｓ５１６でＹｅｓ）は、（９）公開鍵証明書（ＰＫＣ）を公開鍵暗号処理部に渡し（Ｓ５１６）、ＩＤＲＡ（個人識別証明書（ＩＤＣ）を発行する登録局）への接続準備を行い（Ｓ５１７）、個人識別証明書（ＩＤＣ）の発行に必要な情報を入力する（Ｓ５１８）。

【０３０７】

公開鍵証明書（ＰＫＣ）を外部機関である認証局（ＣＡ）から取得して受信することを望む場合（Ｓ５２０）、既に登録済みの公開鍵証明書（ＰＫＣ）の有無を判定（Ｓ５２１）し、ある場合は、その公開鍵証明書（ＰＫＣ）を認証局（ＣＡ）から取得してユーザデバイスに格納する（Ｓ５２２）。

【０３０８】

登録済みの公開鍵証明書（ＰＫＣ）が無い場合は、新規発行処理となり、公開鍵、秘密鍵の鍵ペアを生成（図６２（５））して、公開鍵証明書（ＰＫＣ）の発行機関であるＲＡ（登録局）に対して新規発行要求（図６２（６）（７））を行なう（Ｓ５２３）。新規に公開鍵証明書（ＰＫＣ）が発行（図６２（８））された場合（Ｓ５２４でＹｅｓ）は、個人識別証明書（ＩＤＣ）とのリンク情報としての組情報を生成して、公開鍵証明書を格納する（Ｓ５２５）。ただし、前述したようにリンク情報の保有形態には、様々な形態があるので、各証明書内部にリンクデータを格納している証明書構成であれば、必ずしも組情報を生成して保存

する処理は必要とされない。

【０３０９】

図６５に示す処理は、ＩＤＲＡ（個人識別証明書（ＩＤＣ）の発行登録受付をする登録局）との接続により、個人識別証明書（ＩＤＣ）の発行を行なう処理である。

【０３１０】

（１０）ユーザデバイスの公開鍵暗号処理部は、ネットワーク接続部へ公開鍵証明書とリンクする個人識別証明書（ＩＤＣ）を獲得するために、ＩＤＲＡのアドレスとサンプリングデータ（あるいは利用者名）を渡す。個人識別証明書（ＩＤＣ）発行に必要なオフライン手続きは予め済ましてあるとする。ＩＤＲＡが要求者のＩＤＣを検索するため使用するオフライン手続きで登録した情報（各種個人情報）と照合するための情報（サンプリングデータ、PIN、氏名など）が別に必要ならば同時にネットワーク接続部へ渡す。

【０３１１】

（１１）ユーザデバイスのネットワーク接続部は、ローカルネットワークやインターネットを介して、ＩＤＲＡにアクセスする（Ｓ５２６）。デバイスとＩＤＲＡとの間で公開鍵証明書ベースの相互認証を行い、セッション鍵を共有するなどして、秘匿通信路を確保する（Ｓ５２７）。ユーザデバイスは、必要な情報（サンプリングデータ、PIN、氏名、住所、電話番号など）もＩＤＲＡに対して送信する。図６２の（１１）－１～８は、ユーザとＩＤＲＡ間でのインタラクティブな通信処理を示す。（１１）－１～４はＩＤＲＡがユーザにデータを送る場合、（１１）－５～８はユーザがＩＤＲＡへデータを送る場合を示す。このデータ送受信においては、必要に応じてセッションキーによる暗号化処理、それぞれの秘密鍵による署名処理、公開鍵による署名検証処理等のデータ検証処理を行なうことが好ましい。発行される個人識別証明書（ＩＤＣ）がユーザデバイスの公開鍵で暗号化したテンプレートを格納する場合には、ユーザデバイスからＩＤＲＡに対して公開鍵（公開鍵証明書）を送付する。

【０３１２】

一連のデータのやり取りが終了すると、ネットワーク接続部は、必要なデータ

、ＩＤＣ発行要求の結果をダウンロードする（Ｓ５３０）。（１２）ＩＤＲＡは、ユーザデバイスから受信したＩＤＣ発行要求を検討し、正当な発行依頼であると判定すると、ＩＤＣの発行手続きを実行するＩＤＣＡに対してＩＤＣの発行要求を行ない、ＩＤＣＡによって発行された個人識別証明書（ＩＤＣ）がＩＤＲＡを介してユーザデバイスに送信される。

【０３１３】

（１３）個人識別証明書（ＩＤＣ）を受信したユーザデバイスは、個人識別証明書（ＩＤＣ）を公開鍵暗号処理部に送信し、（１４）公開鍵暗号処理部は個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）のリンク情報としてのリンク（組）情報を生成（Ｓ５３２）して、リンク（組）情報の更新を実行する（Ｓ５３３）。ただし、前述したようにリンク情報の保有形態には、様々な形態があるので、各証明書内部にリンクデータを格納している証明書構成であれば、必ずしも組情報を生成して保存する処理は必要とされない。これらの処理が終了すると、（１５）ＩＤＣ発行要求処理の結果を入出力機能部を介して表示して処理を終了する（Ｓ５３４，Ｓ５３５）。

【０３１４】

ステップＳ５３６、Ｓ５３７は、個人識別証明書（ＩＤＣ）の発行処理が拒否された場合の処理であり、この場合、ユーザデバイスは、入出力機能部を介して処理失敗を通知して処理を終了する。また、ステップＳ５３８，Ｓ５３９は、新規の公開鍵証明書（ＰＫＣ）の発行が拒否された場合の処理であり、この場合、ユーザデバイスは、入出力機能部を介して処理失敗を通知して処理を終了する。

【０３１５】

［９．ワンタイム公開鍵証明書（ワンタイムＰＫＣ）］

次に、個人識別認証局（ＩＤＡ）のテンプレートを用いた個人認証に基づいて、認証局（ＣＡ）が、公開鍵証明書（ＰＫＣ）を発行する処理形態について説明する。以下、この形態で発行される公開鍵証明書をワンタイムＰＫＣと呼ぶ。ワンタイムＰＫＣは、例えば取引のないサービスプロバイダとの間において、コンテンツ取得等の取引を行ないたい場合に、既に個人識別認証局（ＩＤＡ）に登録されている個人識別証明書（ＩＤＣ）に基づいて個人認証を実行し、認証局（Ｃ

Ａ）による厳格な審査手続きを省略した形で発行される公開鍵証明書である。正式な公開鍵証明書の位置づけとはならず、特定の取り引き、例えば１回限りの取り引きにおいて有効とみなされる公開鍵証明書である。

【０３１６】

図６６にワンタイムＰＫＣの発行手順を説明する図を示す。図中の番号順に処理が進行する。図６７は、詳細なワンタイムＰＫＣの発行手順を示すフロー図である。図６６，６７に基づいてワンタイムＰＫＣの発行処理を説明する。

【０３１７】

まず、ワンタイムＰＫＣの発行要求を持つユーザは、認証要求装置に指紋データ等のサンプリングデータを入力（図６７，Ｓ２０１）する。認証要求装置は、機器内で、サンプリングデータを入力したユーザの公開鍵、秘密鍵のペアをワンタイムＰＫＣ用の鍵セットとして生成する（Ｓ２０２）。

【０３１８】

次に、認証要求装置は、個人識別認証局（ＩＤＡ）との間で相互認証処理を実行し（Ｓ２０３）、認証成立を条件として、サンプリングデータ、生成した公開鍵、ユーザ識別データを送信する。送信データは、セッションキーで暗号化を行ない、さらに署名処理を実行して送付することが望ましい。

【０３１９】

認証要求装置からデータを受信した個人識別認証局（ＩＤＡ）は受信サンプリングデータと、ユーザ識別データから識別されるユーザの予め登録済みの個人識別証明書（ＩＤＣ）からテンプレートを抽出して、照合処理を実行する（Ｓ２０５）。次に、個人識別認証局（ＩＤＡ）は、データベースからユーザＩＤを取り出し（Ｓ２０６）、個人識別認証局（ＩＤＡ）と認証局（ＣＡ）との間で相互認証処理を実行し（Ｓ２０７）、認証成立を条件として、認証局（ＣＡ）にユーザＩＤと公開鍵を送信する（Ｓ２０８）。この場合の送信データについても暗号化、署名処理がなされることが望ましい。

【０３２０】

認証局（ＣＡ）は、受信した公開鍵に対応する公開鍵証明書をワンタイムＰＫＣとして生成し、発行履歴を管理する（Ｓ２０９，２１０）する。認証局（ＣＡ

）は、生成したワンタイムＰＫＣを個人識別認証局（ＩＤＡ）を介して認証要求装置に送付する（Ｓ２１１）。

【０３２１】

認証要求装置は、受信したワンタイムＰＫＣを用い、例えばサービスプロバイダに対するサービスリクエストを実行する（Ｓ２１２，２１３）。具体的には、例えばコンテンツ要求データ、あるいは決済要求データ等の要求データに生成した秘密鍵による署名を付加し、公開鍵証明書（ワンタイムＰＫＣ）と併せてサービスプロバイダに送信する。

【０３２２】

サービスプロバイダは、受信データから公開鍵証明書（ワンタイムＰＫＣ）を取り出し、ユーザの公開鍵を抽出して、公開鍵を用いて署名検証を実行し、サービスリクエスト検証処理を行なう（Ｓ２１４）。検証がＯＫであれば、サービスを提供する（Ｓ２１５）。サービスを受領した認証要求装置は、装置内で生成した公開鍵、秘密鍵、および発行されたワンタイムＰＫＣの削除（Ｓ２１６）を行なう。なお、公開鍵、秘密鍵は削除せず、公開鍵証明書であるワンタイムＰＫＣのみを削除する処理構成としてもよい。

【０３２３】

図６７に示す一連の処理、すなわち、Ｓ２０１のサンプリングデータ送信から、Ｓ２１６のデータ削除処理までの処理は、一連の処理を自動的に実行する特定の処理プログラム、例えばサービスプロバイダによって提供されるプログラムに基づいて実行される。従って、個人認証要求装置に送信されてきたワンタイムＰＫＣは、処理の完結により個人認証要求装置から削除され、ＰＫＣの他の取り引きにおける流用が防止されるものとなっている。ただし、必ずしも削除処理を要求されるものではなく、特定の限定された取り引きにおいて、ワンタイムＰＫＣを繰り返し使用可能とする形態としてもよい。

【０３２４】

このように、公開鍵証明書（ワンタイムＰＫＣ）の発行要求者の個人識別データとしてのテンプレートを個人識別証明書から取得し、テンプレートとサンプリング情報との照合処理により個人認証を実行し、個人認証の成立を条件として、

要求者の公開鍵証明書を発行する構成としたので、公開鍵証明書の発行手続きが簡素化され、迅速な公開鍵証明書発行処理が可能となる。

【０３２５】

さらに、個人認証処理を個人識別認証局において実行し、公開鍵証明書（ワンタイムＰＫＣ）を発行する認証局においては、個人識別認証局の個人認証の成立を条件として公開鍵証明書を発行することが可能となるので、認証局における個人確認処理負担が軽減される。

【０３２６】

さらに、個人識別認証局によるユーザサンプリング情報と個人識別証明書の格納テンプレートとの照合処理による個人認証成立を条件として、ユーザに対して発行される公開鍵証明書（ワンタイムＰＫＣ）は、公開鍵証明書（ワンタイムＰＫＣ）を受領した情報処理装置における公開鍵証明書の利用処理完了に伴い削除処理が実行されるので、個人識別認証局の個人認証に基づく公開鍵証明書（ワンタイムＰＫＣ）特有の処理においてのみ利用可能な構成が実現される。

【０３２７】

［１０．照合証明書］

個人識別認証局（ＩＤＡ）は、個人識別証明書のテンプレートとサンプリング情報との照合により、両データが一致した場合は、サンプリング情報を提供した個人が個人識別証明書に対応する個人であることを認証する。これまでに説明した例では、照合の結果について照合ＯＫまたはＮＧの通知を行なうものとして説明してきたが、個人識別認証局（ＩＤＡ）は、認証したことを示す証明書として照合証明書を発行する構成としてもよい。以下、照合証明書の発行処理について説明する。

【０３２８】

図６８に、照合証明書の第１の利用形態を説明する図を示す。図中の番号１～１０の順で処理が進行する。さらに、細かく手続きを説明したフローを図６９に示す。図６８，６９を用いて処理を説明する。

【０３２９】

まず、個人認証処理を行なおうとするユーザは、サンプリングデータを個人認

証要求装置に送信する（図６９，Ｓ１０１）。ここでの個人認証要求装置は、例えばユーザデバイスまたは、サービスプロバイダの通信可能なシステムである。

【０３３０】

次に、個人認証要求装置は、個人識別認証局（ＩＤＡ）との間で相互認証処理を実行（Ｓ１０２）し、認証成立を条件として個人認証要求装置はサンプリングデータと個人認証要求装置の識別子（ＩＤ）を個人識別認証局（ＩＤＡ）に送信（Ｓ１０３）する。この際のデータ送信は、認証処理において生成したセッションキー、あるいは個人識別認証局（ＩＤＡ）の公開鍵で暗号化して送信する。認証が不成立の場合は、エラー処理（Ｓ１２２）とし、以下の処理は実行しない。

【０３３１】

次に、個人識別認証局（ＩＤＡ）は、自己のデータベースに格納されている認証対象者の個人識別証明書（ＩＤＣ）のテンプレートを取り出して、受信したサンプリングデータとの照合を実行（Ｓ１０４）する。照合が不一致であった場合は、以下の手続きは実行されない。

【０３３２】

次に、個人識別認証局（ＩＤＡ）は、自己のデータベースに格納されている認証対象者の識別子（ＩＤ）を取り出し（Ｓ１０５）、照合の成立した個人のＩＤに基づいて照合証明書を生成する（Ｓ１０６）。さらに、照合証明書の発行履歴、例えば証明書の発行日時、有効期間管理データを生成して格納する（Ｓ１０７）。その後、個人識別認証局（ＩＤＡ）は、照合証明書を、個人認証要求装置に対して発行する。

【０３３３】

以下の処理は、発行された照合証明書を利用してサービスプロバイダに対してサービス提供の要求を行なう場合の処理である。照合証明書の発行を受けたユーザは、照合証明書と、サービス要求データ等の電文に署名を付加し、さらに、公開鍵証明書を添付してサービスリクエストをサービスプロバイダに対するリクエストとして生成（Ｓ１０９）し、サービスプロバイダに対して送信する（Ｓ１１０）。

【０３３４】

サービスプロバイダは、受信した公開鍵証明書から、公開鍵を取り出して、署名を検証し（Ｓ１１１）、データ改竄のないことを条件として、ユーザにサービスを提供する（Ｓ１１２）。さらに、サービスを受信した個人認証要求装置は、照合証明書を削除する（Ｓ１１３）。

【０３３５】

図６９に示す一連の処理、すなわち、Ｓ１０１のサンプリングデータ送信から、Ｓ１１３の照合証明書削除処理までの処理は、一連の処理を自動的に実行する特定の処理プログラム、サービスプロバイダによって提供されるプログラムに基づいて実行される。従って、個人認証要求装置に送信されてきた照合証明書は、処理の完結により個人認証要求装置から削除され、証明書の流用が防止されるものとなっている。ただし、必ずしも削除処理を要求されるものではなく、例えば特定の限定された取り引きにおいて、照合証明書を繰り返し使用可能とする形態としてもよい。

【０３３６】

図７０に示す照合証明書利用態様（２）は、図６８の例と異なり、サービスプロバイダが、サービス提供ユーザの照合証明書を取得する処理構成である。

【０３３７】

サービスプロバイダに対してサービス提供を要求するユーザは、認証要求装置において、サービスリクエストおよび指紋データ等のサンプリングデータを構成要素とするリクエストデータを生成し、署名を実行する。次に、認証要求装置とサービスプロバイダ間で相互認証を実行し、認証成立を条件として、生成リクエストデータを送信する。

【０３３８】

リクエストデータを受信したサービスプロバイダは、署名を検証して、データ改竄チェックを実行し、改竄のないことを確認の後、個人識別認証局（ＩＤＡ）との間で相互認証処理を実行し、ユーザから受信したサンプリングデータと認証要求装置のＩＤを、サービスプロバイダの署名を付けて送信する。

【０３３９】

個人識別認証局（ＩＤＡ）は、受信データの検証を行ない、データ改竄のない

ことを確認して、受信サンプリングデータとテンプレートとの照合処理を実行し、照合成立を条件として照合証明書を生成し、発行履歴を生成、格納する。

【０３４０】

生成した照合証明書は、サービスプロバイダに送付され、サービスプロバイダは照合証明書により、サービス要求ユーザの認証がなされたとの判定を行ない、認証要求装置、ユーザに対してサービス提供のＯＫを通知する。サービスプロバイダは、照合証明書を削除して処理を終了する。

【０３４１】

図７１に照合証明書のフォーマット例を示す。各データ項目について説明する。

【０３４２】

バージョン（version）は、照合証明書フォーマットのバージョンを示す。

認証番号（Serial Number）は、個人識別認証局（ＩＤＡ）によって設定される各照合証明書のシリアルナンバである。

署名方式（Signature algorithm Identifier algorithm parameter）は、照合証明書の署名アルゴリズムとそのパラメータを記録するフィールドである。なお、署名アルゴリズムとしては、楕円曲線暗号およびＲＳＡがあり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、ＲＳＡが適用されている場合には鍵長が記録される。

発行者（issuer）は、照合証明書の発行者、すなわち個人識別認証局（ＩＤＡ）の名称が識別可能な形式（Distinguished Name）で記録されるフィールドである。

有効期限(validity)は、証明書の有効期限である開始日時、終了日時が記録される。

サブジェクト(subject)は、ユーザである認証対象者の名前が記録される。具体的には例えばユーザのＩＤや、氏名等である。

個人識別証明書情報（Subject IDA Info）は、ユーザの個人識別証明書情報として、例えば個人識別証明書の認証番号、認証者固有ＩＤ等の各情報が格納される。

公開鍵証明書情報（Subject PKC info）には、被認証者の公開鍵証明書情報としての、被認証者の公開鍵証明書の認証番号、被認証者の公開鍵証明書の被認証者固有ＩＤが格納される。

電子署名は、証明書を構成する各フィールドの全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して個人識別認証局（ＩＤＡ）の秘密鍵を用いて生成したデータである。

【０３４３】

上述のように、照合証明書には、公開鍵証明書、個人識別証明書とリンクが張れるように、公開鍵証明書情報、個人識別証明書情報が含まれている。また、被認証者識別データが含まれている。

【０３４４】

［１１．個人識別証明書（ＩＤＣ）のダウンロードおよびコンテンツ利用処理］

次に、ユーザの個人識別証明書（ＩＤＣ）が格納されていないデバイスを使用してコンテンツの配信等の際に、個人識別認証局（ＩＤＡ）に登録済みの個人識別証明書（ＩＤＣ）を利用して個人認証を実行し、コンテンツ配信等のサービスを受ける処理について説明する。

【０３４５】

音楽データ、画像データ等の様々なコンテンツをサービスプロバイダから受信しようとするユーザは、１つのユーザ端末（ユーザデバイス）を使用するとは限らず、複数のデバイスを使用する場合がある。例えば自宅のデバイス、会社のデバイス、あるいは不特定多数が利用可能なデバイス等である。

【０３４６】

上述した個人識別証明書（ＩＤＣ）を使用した個人認証を実行するためには、個人識別証明書に対するアクセスが必要となる。例えばユーザＡが頻繁に利用するユーザデバイスに個人識別証明書（ＩＤＣ）が格納されていれば、その格納ＩＤＣを用いて個人認証がそのデバイスにおいて実行可能であるが、会社のデバイス、あるいは不特定多数が利用可能なデバイスに、そのデバイスを利用するすべてのユーザの個人識別証明書（ＩＤＣ）を格納することは現実的でない。このよ

うな状況にあるデバイスにおいて、個人識別認証局（ＩＤＡ）に登録済みの個人識別証明書（ＩＤＣ）を利用して個人認証を行ない、さらにその個人認証処理に基づいてコンテンツ配信を受ける処理について、以下説明する。

【０３４７】

図７２に、個人識別認証局（ＩＤＡ）に登録済みの個人識別証明書（ＩＤＣ）を利用して個人認証を行ない、さらに、個人認証処理に基づいてコンテンツ配信を受ける処理を説明する図を示す。図中の番号１～１１の順で処理が進行する。さらに、詳細な手続きを説明したフローを図７３～図７５に示す。図７２、および図７３～図７５を用いて処理を説明する。

【０３４８】

図７２に示すように、ユーザＡは、通常は、ユーザＡのデバイスＡを用いて処理、例えばコンテンツの受信等の処理を実行する。従ってデバイスＡには、コンテンツの配信を実行するするために必要な各種の証明書、すなわちユーザＡの公開鍵証明書（ＰＫＣ）、個人識別証明書（ＩＤＣ）、さらに、デバイスＡの公開鍵証明書（ＰＫＣ）が格納されている。ユーザＡは必要に応じて、各種ＰＫＣを用いて相互認証処理を実行し、また、ＩＤＣを用いて個人認証処理が実行可能である。

【０３４９】

ここで、ユーザＡが、他のデバイス、図７２に示す例では、ユーザＢのデバイスＢを使用してコンテンツ配信等のサービスを受ける場合を考える。デバイスＢには、ユーザＢの公開鍵証明書（ＰＫＣ）、個人識別証明書（ＩＤＣ）、さらに、デバイスＢの公開鍵証明書（ＰＫＣ）が格納されている。ユーザＢは、これらの証明書を利用して相互認証、個人認証処理が実行可能であるが、ユーザＡは、デバイスＢに格納された各証明書のみでは、個人認証、または相互認証が実行できない場合がある。このようなデバイスＢにおいてユーザＡがＩＤＣを利用した個人認証、ＰＫＣを利用した相互認証を実行してコンテンツの配信サービスを実行する処理を図７３以下のフローを用いて説明する。

【０３５０】

まず、デバイスＢを利用するユーザＡは、デバイスＢにアクセス（起動）する

（Ｓ８０１）。デバイスＢは、デバイスＢに対するアクセス許可のあるユーザによるアクセスであるか否かを判定するために、個人認証処理を開始（Ｓ８０２）し、ユーザＡに対してサンプリング情報の入力を要求する。ユーザＡは、デバイスＢにユーザＩＤと指紋等のサンプリング情報を入力（Ｓ８０３）すると、デバイスＢは、ユーザＩＤ、またはサンプリング情報に基づいてデバイス内の記憶手段の格納ＩＤＣの検索を実行（Ｓ８０４）する。デバイスＢには、ユーザＡに対応するＩＤＣは格納されていないので、ＩＤＣは検出されない。この場合、デバイスＢは、ユーザＡのＩＤＣを個人識別認証局（ＩＤＡ）に要求する。この際、デバイスＢは、個人識別認証局（ＩＤＡ）との間で相互認証を実行し、セッションキーを生成してセッションキーによる暗号化を行なったユーザＡのユーザＩＤ、サンプリング情報を個人識別認証局（ＩＤＡ）に送信する。

【０３５１】

次に、個人識別認証局（ＩＤＡ）は、自己のデータベースに格納されているユーザＡの個人識別証明書（ＩＤＣ）を取り出して、デバイスＢに送信する。なお、この場合、個人識別証明書（ＩＤＣ）内に格納するテンプレート情報は、デバイスＢにおいて利用可能な形態、具体的にはデバイスＢの公開鍵で暗号化してＩＤＣに格納する。デバイスＢは受信したユーザＡの個人識別証明書（ＩＤＣ）をデバイス内のメモリに格納する（Ｓ８０６）。

【０３５２】

デバイスＢは、メモリに格納したユーザＡの個人識別証明書（ＩＤＣ）を用いてサンプリングデータとの照合を実行、すなわち個人認証処理を行なう（Ｓ８０７）。照合が不一致であった場合は、エラーとなり、以下の手続きは実行されない。

【０３５３】

個人認証が成立すると、デバイスＢは、サービスプロバイダの提供するサービスに適用可能な公開鍵・秘密鍵のペアを検索（Ｓ８０９）する。なお、サービスプロバイダは、各ユーザとの間のデータ通信において、予め各ユーザ毎、あるいはデバイス毎に設定された公開鍵・秘密鍵のペアを用いて相互認証等、各種の暗号化処理を実行するものとする。ここでは、ユーザＡ専用の公開鍵・秘密鍵のペ

アは、デバイスＢに格納されておらず、ステップＳ８１０の判定はＮｏとなり、デバイスＢにおいて、新たな公開鍵・秘密鍵のペアを生成する（Ｓ８１１）。

【０３５４】

次にデバイスＢは、生成した公開鍵を認証局（ＣＡ）に送信し、公開鍵証明書の発行手続きを実行して、ユーザＡの公開鍵証明書（ＰＫＣ）を取得し、デバイスＢに格納する（Ｓ８１２）。

【０３５５】

次に、デバイスＢは、ユーザＡの個人識別証明書（ＩＤＣ）と、公開鍵証明書（ＰＫＣ）のリンクを形成する。リンクは例えば前述の組情報を生成してメモリに格納する処理として実行する。この際、リンク（組情報）に対してそのＩＤＣ，ＰＫＣを適用して利用可能なサービス名を対応付けて登録する（Ｓ８１３）。すなわち、いずれのサービスプロバイダまたはコンテンツプロバイダからのサービスに適用可能なＩＤＣ，ＰＫＣセットであるかを対応付けて、例えばプロバイダ識別子またはサービス識別子等の処理識別子を併せて登録する。

【０３５６】

次に、デバイスＢは、ユーザＡの公開鍵証明書（ＰＫＣ）を用いて、サービス登録サーバと相互認証を実行（Ｓ８１４）する。なお、サービス登録サーバは、管轄する1以上のサービスプロバイダ（コンテンツ配信サーバ等）のサービスを提供するユーザのユーザ登録を行なうサーバであり、各ユーザの公開鍵証明書（ＰＫＣ）を登録することにより、管轄下のサービスプロバイダのサービス実行時の認証処理等、各種暗号処理を登録ＰＫＣを用いて実行可能としたサーバである。

【０３５７】

サービス登録サーバとの相互認証が成立すると、次にサービス登録サーバに対するユーザＡの個人認証をユーザＡの個人識別証明書（ＩＤＣ）を用いて実行する（Ｓ８１６）。これらの処理が済むと、サービス登録サーバは、ユーザＡの公開鍵証明書（ＰＫＣ）を登録（Ｓ８１８）する。なお、個人認証処理は必要に応じて実行すればよく、必須ではない。例えばコンテンツ配信時にコンテンツ配信サーバとの間で個人認証を行なってもよい。

【０３５８】

デバイスＢは、サービス登録サーバからユーザＡの公開鍵証明書（ＰＫＣ）の登録終了通知を受領し、登録したユーザＡの公開鍵証明書（ＰＫＣ）を用いて利用可能なサービス情報、コンテンツ配信サーバのＰＫＣを受信（Ｓ８１９）する。

【０３５９】

以下の処理は、コンテンツ配信サーバからのコンテンツ配信を実行する処理であり、ステップＳ８２０でコンテンツ配信サーバのＰＫＣとユーザＡのＰＫＣとを用いて、相互認証処理を実行し、相互認証の成立を条件としてコンテンツの配信を受ける（Ｓ８２２）。なお、コンテンツ配信サーバは、デバイスＢからのコンテンツ要求に応じて、コンテンツ要求の際の相互認証に用いられたＰＫＣがコンテンツ利用権のあるＰＫＣとしてサービス登録サーバに登録されているか否かを確認する処理を実行する。確認が取れた場合にのみコンテンツの配信を行なう。サービス登録サーバには、ユーザＡの公開鍵証明書（ＰＫＣ）が登録済みであるので、コンテンツ要求は承認され、コンテンツが配信されることになる。

【０３６０】

このように、デバイスに、ユーザの個人識別証明書（ＩＤＣ）、公開鍵証明書（ＰＫＣ）が格納されていない場合であっても、ユーザは、個人識別認証局（ＩＤＡ）に登録されたＩＤＣをデバイスにダウンロードし、さらにデバイスにおいて生成した公開鍵・秘密鍵のペアに基づいて認証局（ＣＡ）から公開鍵証明書（ＰＫＣ）を受領し、ＩＤＣに基づく個人認証、ＰＫＣに基づく相互認証、データ暗号化処理を実行し、サービスプロバイダからのサービス提供を受領することが可能となる。

【０３６１】

以上が、ユーザ個人に対して設定された個人識別証明書（ＩＤＣ）、公開鍵証明書（ＰＫＣ）を用いた処理である。次にユーザ個人に対して設定された個人識別証明書（ＩＤＣ）と、デバイスに対して設定された公開鍵証明書（ＰＫＣ）を用いた処理について説明する。

【０３６２】

図７６に、ユーザ個人に対して設定された個人識別証明書（ＩＤＣ）と、デバイスに対して設定された公開鍵証明書（ＰＫＣ）を用い、個人識別認証局（ＩＤＡ）に登録済みの個人識別証明書（ＩＤＣ）を利用して個人認証を行ない、デバイスに対して設定された公開鍵証明書（ＰＫＣ）に基づいてコンテンツ配信を受ける処理を説明する図を示す。図中の番号１～６の順で処理が進行する。さらに、詳細な手続きを説明したフローを図７７～図７８に示す。図７６、および図７７～図７８を用いて処理を説明する。

【０３６３】

図７６に示すように、ユーザＡは、通常は、ユーザＡのデバイスＡを用いて処理、例えばコンテンツの受信等の処理を実行する。従ってデバイスＡには、コンテンツの配信を実行するするために必要な各種の証明書、すなわちユーザＡの公開鍵証明書（ＰＫＣ）、個人識別証明書（ＩＤＣ）、さらに、デバイスＡの公開鍵証明書（ＰＫＣ）が格納されている。ユーザＡは必要に応じて、各種ＰＫＣを用いて相互認証処理を実行し、また、ＩＤＣを用いて個人認証処理が実行可能である。

【０３６４】

ここで、ユーザＡが、他のデバイス、図７６に示す例では、ユーザＢのデバイスＢを使用してコンテンツ配信等のサービスを受ける場合を考える。デバイスＢには、ユーザＢの個人識別証明書（ＩＤＣ）、さらに、デバイスＢの公開鍵証明書（ＰＫＣ）が格納されている。ユーザＢは、これらの証明書を利用して相互認証、個人認証処理が実行可能であるが、ユーザＡは、デバイスＢに格納された各証明書のみでは、個人認証が実行できない。このようなデバイスＢにおいてユーザＡがＩＤＣを利用した個人認証、ＰＫＣを利用した相互認証を実行してコンテンツの配信サービスを実行する処理を図７７以下のフローを用いて説明する。

【０３６５】

まず、デバイスＢを利用するユーザＡは、デバイスＢにアクセス（起動）する（Ｓ８５１）。デバイスＢは、デバイスＢに対するアクセス許可のあるユーザによるアクセスであるか否かを判定するために、個人認証処理を開始（Ｓ８５２）し、ユーザＡに対してサンプリング情報の入力を要求する。ユーザＡは、デバイ

スＢにユーザＩＤと指紋等のサンプリング情報を入力（Ｓ８５３）すると、デバイスＢは、ユーザＩＤ、またはサンプリング情報に基づいて格納ＩＤＣの検索を実行（Ｓ８５４）する。デバイスＢには、ユーザＡに対応するＩＤＣは格納されていないので、ＩＤＣは検出されない。この場合、デバイスＢは、ユーザＡのＩＤＣを個人識別認証局（ＩＤＡ）に要求する。この際、デバイスＢは、個人識別認証局（ＩＤＡ）との間で相互認証を実行し、セッションキーを生成してセッションキーによる暗号化を行なったユーザＡのユーザＩＤ、サンプリング情報を個人識別認証局（ＩＤＡ）に送信する。

【０３６６】

次に、個人識別認証局（ＩＤＡ）は、自己のデータベースに格納されているユーザＡの個人識別証明書（ＩＤＣ）を取り出して、デバイスＢに送信する。なお、この場合、個人識別証明書（ＩＤＣ）内に格納するテンプレート情報は、デバイスＢにおいて利用可能な形態、具体的にはデバイスＢの公開鍵で暗号化してＩＤＣに格納する。デバイスＢは受信したユーザＡの個人識別証明書（ＩＤＣ）をデバイス内のメモリに格納する（Ｓ８５６）。

【０３６７】

デバイスＢは、メモリに格納したユーザＡの個人識別証明書（ＩＤＣ）を用いてサンプリングデータとの照合を実行、すなわち個人認証処理を行なう（Ｓ８５７）。照合が不一致であった場合は、エラーとなり、以下の手続きは実行されない。

【０３６８】

個人認証が成立すると、デバイスＢは、サービスプロバイダの提供するサービスに適用可能な公開鍵・秘密鍵のペアを検索（Ｓ８５９）する。なお、サービスプロバイダは、各ユーザとの間のデータ通信において、予め各ユーザ毎、あるいはデバイス毎に設定された公開鍵・秘密鍵のペアを用いて相互認証等、各種の暗号化処理を実行するものとする。ここでは、デバイスＢの公開鍵・秘密鍵のペアが適用可能な設定である。デバイスＢは、デバイスＢの公開鍵証明書（ＰＫＣ）を用いて、サービス登録サーバと相互認証を実行（Ｓ８６０）する。なお、サービス登録サーバは、管轄する1以上のサービスプロバイダ（コンテンツ配信サー

バ等）のサービスを提供するユーザのユーザ登録を行なうサーバであり、各ユーザの公開鍵証明書（ＰＫＣ）を登録することにより、管轄下のサービスプロバイダのサービス実行時の認証処理等、各種暗号処理を登録ＰＫＣを用いて実行可能としたサーバである。ここでは、サービス登録サーバは、各デバイスの公開鍵証明書（ＰＫＣ）、または各デバイスの公開鍵証明書（ＰＫＣ）と各ユーザの個人識別証明書（ＩＤＣ）を登録するものとする。

【０３６９】

サービス登録サーバとの相互認証が成立すると、次にサービス登録サーバに対するユーザＡの個人認証をユーザＡの個人識別証明書（ＩＤＣ）を用いて実行する（Ｓ８６２）。これらの処理が済むと、デバイスＢは、サービス登録サーバからサービス利用可能通知を受領し、利用可能なサービス情報、コンテンツ配信サーバのＰＫＣを受信する（Ｓ８６４）。

【０３７０】

以下の処理は、コンテンツ配信サーバからのコンテンツ配信を実行する処理であり、ステップＳ８６５でコンテンツ配信サーバのＰＫＣとデバイスＢのＰＫＣとを用いて、相互認証処理を実行し、相互認証の成立を条件としてコンテンツの配信を受ける（Ｓ８６７）。なお、コンテンツ配信サーバは、デバイスＢからのコンテンツ要求に応じて、コンテンツ要求の際の相互認証に用いられたＰＫＣがコンテンツ利用権のあるＰＫＣとしてサービス登録サーバに登録されているか否かを確認する処理を実行する。確認が取れた場合にのみコンテンツの配信を行なう。サービス登録サーバには、デバイスＢの公開鍵証明書（ＰＫＣ）が登録済みであるので、コンテンツ要求は承認され、コンテンツが配信されることになる。

【０３７１】

このように、デバイスに、ユーザの個人識別証明書（ＩＤＣ）、公開鍵証明書（ＰＫＣ）が格納されていない場合であっても、ユーザは、個人識別認証局（ＩＤＡ）に登録されたＩＤＣをデバイスにダウンロードし、さらにデバイスに格納されたデバイスの公開鍵証明書（ＰＫＣ）を用いて、ＩＤＣに基づく個人認証、ＰＫＣに基づく相互認証、データ暗号化処理を実行し、サービスプロバイダからのサービス提供を受領することが可能となる。

【０３７２】

［１２．個人識別証明書（ＩＤＣ）の有効期限設定］

これまで、説明してきたように、個人識別証明書（ＩＤＣ）は個人を識別するためのテンプレート情報、例えば指紋情報、パスワード等、個人情報を格納している。このテンプレート情報は暗号化されているものの、暗号解読、改竄の可能性が全くゼロであるとは言えず、管理されないない個人識別証明書（ＩＤＣ）が氾濫する結果を招くことは好ましいとはいえない。従って、個人識別認証局（ＩＤＡ）により発行され、ユーザデバイス（ＵＤ）、あるいはサービスプロバイダ（ＳＰ）において使用される個人識別証明書（ＩＤＣ）の管理が重要となる。

【０３７３】

ここでは、個人識別証明書（ＩＤＣ）にＩＤＣ自体の有効情報として、ＩＤＣの有効期限、有効利用回数を設定し、さらに、個人識別証明書（ＩＤＣ）に格納したテンプレート情報の有効期限を設定することにより、ＩＤＣおよびテンプレートが無限に使用可能な状態となることを防止するＩＤＣ管理構成について説明する。有効期限の設定により、例えば定期的なユーザ審査が可能となり、また、個人識別証明書（ＩＤＣ）の発行対象者に対する有効性確認が容易となる。

【０３７４】

図７９に、個人識別証明書（ＩＤＣ）の有効情報（有効期限および有効利用回数）と、ＩＤＣに格納したテンプレート情報の有効期限とを設定した個人識別証明書構成を示す。個人識別認証局（ＩＤＡ）１００１は、ユーザの個人識別証明書（ＩＤＣ）を発行し、個人認証処理実行エンティテイであるサービスプロバイダ（ＳＰ）１００２，ユーザ端末１００３に配布する。サービスプロバイダ（ＳＰ）１００２，ユーザ端末１００３においては、ＩＤＡから発行された個人識別証明書（ＩＤＣ）を格納し、ユーザから入力されるサンプリング情報との照合処理を実行して個人認証を行なう。

【０３７５】

個人識別認証局（ＩＤＡ）１００１により発行される個人識別証明書（ＩＤＣ）には、図に示すように［利用有効期限または有効回数］１００４、［テンプレート有効期限］１００５、が格納され、全体に個人識別認証局（ＩＤＡ）の秘密

鍵による署名１００６がなされている。署名１００６は、個人識別証明書（ＩＤＣ）を受領したサービスプロバイダ１００２、ユーザデバイス１００３において、個人識別認証局（ＩＤＡ）１００１の公開鍵を用いて検証され、個人識別証明書（ＩＤＣ）の改竄の有無がチェックされる。

【０３７６】

個人識別証明書（ＩＤＣ）に格納された［利用有効期限または有効回数］１００４は、ＩＤＣ自体の有効期限を定めたデータである。これらは、個人識別証明書（ＩＤＣ）の発行主体である個人識別認証局（ＩＤＡ）１００１により設定され、ＩＤＣに格納される。個人識別認証局（ＩＤＡ）１００１は、同一のユーザのテンプレート情報を格納したＩＤＣであっても、提供先となるサービスプロバイダ、またはユーザデバイスに応じて異なる［利用有効期限、有効回数］を設定したＩＤＣを作成して提供することができる。ＩＤＣを用いた個人認証を実行するサービスプロバイダ、またはユーザデバイスでは、サンプリング情報との照合を実行する前に個人識別証明書（ＩＤＣ）に格納された［利用有効期限または有効回数］を検証し、指定期限、指定回数を満足している場合にのみ、照合処理を実行する。

【０３７７】

個人識別証明書（ＩＤＣ）に格納された［テンプレート有効期限］１００５は、ＩＤＣに格納されたテンプレート情報の有効期限を定めたデータである。これらは、個人識別証明書（ＩＤＣ）の発行主体である個人識別認証局（ＩＤＡ）１００１により設定されるか、あるいはテンプレート情報の元データである個人データを提供したユーザ自体が設定する。ユーザがテンプレート情報の有効期限を設定する場合は、個人識別データとともに、有効期限情報を個人識別認証局（ＩＤＡ）１００１に送付し、個人識別認証局（ＩＤＡ）１００１が受領した有効期限情報に基づいてテンプレート情報の有効期限を設定してＩＤＣに格納する。ＩＤＣを用いた個人認証を実行するサービスプロバイダ、またはユーザデバイスでは、サンプリング情報とＩＤＣ内のテンプレートとの照合を実行する前に個人識別証明書（ＩＤＣ）に格納された［利用有効期限または有効回数］を検証するとともに、テンプレート情報の［テンプレート有効期限］を検証し、指定期限を満

足している場合にのみ、照合処理を実行する。

【０３７８】

図８０に個人識別証明書（ＩＤＣ）に格納された［利用有効期限または有効回数］、およびテンプレート情報の［テンプレート有効期限］の管理構成を説明する図を示す。図８０（ａ）は、ＩＤＣの有効期限１０１４と、テンプレートの有効期限１０１５を格納した例であり、図８０（ｂ）は、ＩＤＣの有効利用回数１０１７と、テンプレートの有効期限１０１５を格納した例である。

【０３７９】

サービスプロバイダ、またはユーザデバイスは、図８０（ａ）のＩＤＣの有効期限１０１４と、テンプレートの有効期限１０１５を格納したＩＤＣを、自己の記憶装置に格納する際は、ＩＤＣの署名１０１６の検証を実行してデータ改竄の無いことを確認した上で格納する。また格納したＩＤＣを用いて個人認証を実行する場合は、ユーザの提供するサンプリング情報との比較処理ステップの前にＩＤＣに格納されたＩＤＣの有効期限１０１４と、テンプレートの有効期限１０１５を検証し、期限内である場合にのみ処理が続行され、期限を過ぎている場合は処理エラーとしてサンプリング情報との照合を実行しない。

【０３８０】

サービスプロバイダ、またはユーザデバイスは、図８０（ｂ）のＩＤＣの有効利用回数１０１７と、テンプレートの有効期限１０１５を格納したＩＤＣを、自己の記憶装置に格納する際は、ＩＤＣの署名１０１６の検証を実行してデータ改竄の無いことを確認した上で格納する。さらに、ＩＤＣに設定されたＩＤＣ利用回数ＳＡＭ内設定情報１０１９を自己のデバイスのＳＡＭ（Secure Application Module）１０２０に格納する。格納データにはＳＡＭの秘密鍵による署名１０１８を行ないデータ改竄を防止する。格納したＩＤＣを用いて個人認証を実行する場合は、ユーザの提供するサンプリング情報との比較処理ステップの前にＩＤＣに格納されたテンプレートの有効期限１０１５を検証し、さらに自己のデバイスのＳＡＭ１０２０に格納されたＩＤＣ利用回数ＳＡＭ内設定情報１０１９を検証し、テンプレートの有効期限が期限内であり、かつＳＡＭに格納されたＩＤＣ利用回数が０でない場合に限り、照合処理が実行され、期限を過ぎている場合、

またはＩＤＣ利用回数が０である場合は処理エラーとしてサンプリング情報との照合を実行しない。サンプリング情報との照合処理が実行された場合は、ＳＡＭに格納されたＩＤＣ利用回数を１減ずる（デクリメント）処理を実行する。

【０３８１】

図８１にＩＤＣ有効期限、テンプレート有効期限の管理構成を説明する図を示す。まず、個人識別証明書（ＩＤＣ）の発行主体である個人識別認証局（ＩＤＡ）１００１は、ＩＤＣ有効期限、テンプレート有効期限の設定ルールを定める。個人識別証明書（ＩＤＣ）の発行を望むユーザは、個人識別認証局（ＩＤＡ）１００１に対してＩＤＣ発行に必要な個人識別情報、個人情報を提供し、個人識別認証局（ＩＤＡ）１００１は、個人確認、データ検証を実行して、正当なＩＤＣ発行要求であることが確認された場合に、新規に個人識別証明書（ＩＤＣ）を生成する。なお、オンラインで処理を実行する際は、相互認証が行われ、通信データに対する署名付加、検証処理が実行される。なお、ユーザがテンプレートの有効期限を自ら設定することを望む場合は、自己の個人情報に加え、設定希望の有効期限をＩＤＡに対して提示し、ＩＤＡは、その有効期限をＩＤＣにテンプレート有効期限として設定する。

【０３８２】

サービスプロバイダ１００２は、ユーザとの取り引きが発生した場合に、ユーザの個人認証を実行するため、個人識別認証局（ＩＤＡ）１００１に対してＩＤＣ発行要求を行なう。個人識別認証局（ＩＤＡ）１００１は、ＩＤＣ有効期限、テンプレート有効期限を設定した個人識別証明書（ＩＤＣ）をサービスプロバイダ１００２に対して発行する。発行する個人識別証明書（ＩＤＣ）には、個人識別認証局（ＩＤＡ）１００１の秘密鍵による署名がなされている。なお、サービスプロバイダ１００２と個人識別認証局（ＩＤＡ）１００１との間の通信処理を実行する際は、相互認証が行われ、通信データに対する署名付加、検証処理が実行される。

【０３８３】

サービスプロバイダ１００２は、自己の所有する個人識別認証局（ＩＤＡ）１００１の公開鍵を用いて署名検証処理を実行した後、ＩＤＣをメモリに格納する

。ユーザの個人認証を行なう場合は、サンプリング情報との比較処理ステップの前にＩＤＣに格納されたＩＤＣの有効期限と、テンプレートの有効期限を検証し、期限内である場合にのみユーザからのサンプリング情報を受領し、照合処理を実行する。なお、図の例では、個人識別証明書（ＩＤＣ）のテンプレート情報は、サービスプロバイダの公開鍵により暗号化されており、サービスプロバイダの秘密鍵により復号を実行してテンプレートをＩＤＣから取り出して照合を実行する。照合が成立した場合には、ユーザの取り引き、例えばコンテンツ提供等を行なう。

【０３８４】

図８２にＩＤＣ有効利用回数、テンプレート有効期限の管理構成を説明する図を示す。まず、個人識別証明書（ＩＤＣ）の発行主体である個人識別認証局（ＩＤＡ）１００１は、ＩＤＣ有効期限、テンプレート有効期限の設定ルールを定める。個人識別証明書（ＩＤＣ）の発行を望むユーザは、個人識別認証局（ＩＤＡ）１００１に対してＩＤＣ発行に必要な個人情報を提供し、個人識別認証局（ＩＤＡ）１００１は、個人確認、データ検証を実行して、正当なＩＤＣ発行要求であることが確認された場合に、新規に個人識別証明書（ＩＤＣ）を生成する。ユーザがテンプレートの有効期限を自ら設定することを望む場合は、自己の個人情報に加え、設定希望の有効期限をＩＤＡに対して提示し、ＩＤＡは、その有効期限をＩＤＣにテンプレート有効期限として設定する。

【０３８５】

サービスプロバイダ１００２は、ユーザとの取り引きが発生した場合に、ユーザの個人認証を実行するため、個人識別認証局（ＩＤＡ）１００１に対してＩＤＣ発行要求を行なう。個人識別認証局（ＩＤＡ）１００１は、ＩＤＣ有効利用回数、テンプレート有効期限を設定した個人識別証明書（ＩＤＣ）をサービスプロバイダ１００２に対して発行する。発行する個人識別証明書（ＩＤＣ）には、個人識別認証局（ＩＤＡ）１００１の秘密鍵による署名がなされている。

【０３８６】

サービスプロバイダ１００２は、自己の所有する個人識別認証局（ＩＤＡ）１００１の公開鍵を用いて署名検証処理を実行した後、ＩＤＣをメモリに格納する

。さらに、ＩＤＣに設定されたＩＤＣ利用回数を自己のデバイスのＳＡＭ（Secure Application Module）に格納する。また格納したＩＤＣを用いて個人認証を実行する場合は、ユーザの提供するサンプリング情報との比較処理ステップの前にＩＤＣに格納されたテンプレートの有効期限を検証し、さらに自己のデバイスのＳＡＭに格納されたＩＤＣ利用回数を検証し、テンプレートの有効期限が期限内であり、かつＳＡＭに格納されたＩＤＣ利用回数が０でない場合に限り、照合処理が実行され、期限を過ぎている場合、またはＩＤＣ利用回数が０である場合は処理エラーとしてサンプリング情報との照合を実行しない。サンプリング情報との照合処理が実行された場合は、ＳＡＭに格納されたＩＤＣ利用回数を１減ずる（デクリメント）処理を実行する。なお、図の例では、個人識別証明書（ＩＤＣ）のテンプレート情報は、サービスプロバイダの公開鍵により暗号化されており、サービスプロバイダの秘密鍵により復号を実行してテンプレートをＩＤＣから取り出して照合を実行する。照合が成立した場合には、ユーザの取り引き、例えばコンテンツ提供等を行なう。

【０３８７】

次に図８３を用いて、個人識別証明書（ＩＤＣ）の［利用有効期限または有効回数］、および［テンプレート有効期限］に基づいたＩＤＣ利用制御処理をまとめて説明する。

【０３８８】

サービスプロバイダ、またはユーザデバイス等においてＩＤＣによる個人認証処理が開始される（Ｓ１００１）と、ユーザはユーザ識別ＩＤと、サンプリングデータを入力または送付する（Ｓ１００２）。個人認証を実行するサービスプロバイダ、またはユーザデバイスは、ユーザＩＤに基づいてＩＤＣ検索を実行し、ＩＤＣの有無を判定し（Ｓ１００３）、ＩＤＣが存在しない場合は、個人識別認証局（ＩＤＡ）に対してＩＤＣ発行要求を出力し、ＩＤＣを取得（Ｓ１００４）する。

【０３８９】

次に、個人識別証明書（ＩＤＣ）の［テンプレート有効期限］情報を取り出してテンプレート有効期限の検証を実行（Ｓ１００５）し、有効期限が有効でない

場合は、個人識別認証局（ＩＤＡ）に対して新たな［テンプレート有効期限］を設定したＩＤＣの発行要求を出力し、ＩＤＣを取得（Ｓ１００６）する。

【０３９０】

次に、個人識別証明書（ＩＤＣ）の［利用有効期限］情報を取り出してＩＤＣ有効期限の検証を実行（Ｓ１００７）し、有効期限が有効でない場合は、個人識別認証局（ＩＤＡ）に対して新たな［利用有効期限］を設定したＩＤＣの発行要求を出力し、ＩＤＣを取得（Ｓ１００８）する。

【０３９１】

次に、個人識別証明書（ＩＤＣ）に［利用有効回数］が設定されているか否かを判定し（Ｓ１００９）、設定されている場合は、自己のデバイスのＳＡＭ内のＩＤＣ利用回数を取り出してＳＡＭ内のＩＤＣ利用回数が０になっているか否かを判定し（Ｓ１０１０）、０である場合は、個人識別認証局（ＩＤＡ）に対して新たな［利用有効回数］を設定したＩＤＣの発行要求を出力し、ＩＤＣを取得（Ｓ１０１１）するとともに、ＳＡＭ内に新規発行されたＩＤＣの利用有効回数を設定（Ｓ１０１２）する。

【０３９２】

次にＩＤＣのテンプレートを取り出し、ユーザの提供したサンプリング情報との照合処理を実行する（Ｓ１０１４）。照合処理終了後、ＩＤＣに有効利用回数が設定されている場合（Ｓ１０１５，Ｙｅｓ）は、ＳＡＭ内の有効利用回数を１デクリメントし（Ｓ１０１６）、さらに、ＳＡＭ内のＩＤＣ利用回数が０になった場合（Ｓ１０１７，Ｙｅｓ）はＳＡＭ内のＩＤＣを消去（Ｓ１０１８）し、照合結果に基づく処理を実行する（Ｓ１０１９）。

【０３９３】

次に、図８４を用い、個人識別証明書（ＩＤＣ）の利用時に、ＩＤＣの［利用有効期限］の期限切れが判明した場合のＩＤＣ更新処理について説明する。

【０３９４】

ユーザの個人識別証明書（ＩＤＣ）が個人識別認証局（ＩＤＡ）１００１により生成され、サービスプロバイダ１００２の要求により、ＩＤＣが個人識別認証局（ＩＤＡ）１００１からサービスプロバイダ１００２に送信され、サービスプ

ロバイダ１００２の記憶手段にＩＤＣが格納されているとする。個人識別証明書（ＩＤＣ）には、［利用有効期限］が設定されている。

【０３９５】

サービスプロバイダ１００２は、ユーザの取り引きにおける個人認証処理の実行時にＩＤＣを取り出し、ＩＤＣ内の［利用有効期限］が期限切れであったことを検出すると、個人識別認証局（ＩＤＡ）１００１に対して、ＩＤＣの発行依頼を実行する。この場合、更新の必要なＩＤＣに対応するユーザＩＤを個人識別認証局（ＩＤＡ）１００１に送信する。なお、データ通信においては、相互認証、署名付加、検証処理が実行される。

【０３９６】

個人識別認証局（ＩＤＡ）１００１は、ユーザＩＤに基づいて、すでに格納済みのユーザテンプレート情報を用いて、新たな有効期限を設定した個人識別証明書（ＩＤＣ）を生成してサービスプロバイダ１００２に送信する。サービスプロバイダは、更新されたＩＤＣを自身の記憶手段に格納し、更新したＩＤＣからテンプレートを取り出し、復号してサンプリング情報との比較照合処理を実行する。

【０３９７】

なお、上述のＩＤＣの有効期限の更新処理は、ＩＤＣの有効利用回数の更新、および個人識別認証局（ＩＤＡ）が設定するテンプレート有効期限の有効性消失時においても同様の手続きが適用可能である。

【０３９８】

図８５に、定期的な個人識別証明書（ＩＤＣ）の期限チェックを実行して、ＩＤＣの［利用有効期限］の期限切れが判明した場合のＩＤＣ更新処理について説明する。

【０３９９】

ユーザの個人識別証明書（ＩＤＣ）が個人識別認証局（ＩＤＡ）１００１により生成され、サービスプロバイダ１００２の要求により、ＩＤＣが個人識別認証局（ＩＤＡ）１００１からサービスプロバイダ１００２に送信され、サービスプロバイダ１００２の記憶手段にＩＤＣが格納されているとする。個人識別証明書

（ＩＤＣ）には、［利用有効期限］が設定されている。

【０４００】

サービスプロバイダ１００２は、定期的に自身の格納した個人識別証明書（ＩＤＣ）の有効期限のチェック処理を実行する。この定期検査時に、ＩＤＣ内の［利用有効期限］が期限切れであったことを検出すると、個人識別認証局（ＩＤＡ）１００１に対して、ＩＤＣの発行依頼を実行する。この場合、更新の必要なＩＤＣに対応するユーザＩＤを個人識別認証局（ＩＤＡ）１００１に送信する。なお、データ通信においては、相互認証、署名付加、検証処理が実行される。

【０４０１】

個人識別認証局（ＩＤＡ）１００１は、ユーザＩＤに基づいて、すでに格納済みのユーザテンプレート情報を用いて、新たな有効期限を設定した個人識別証明書（ＩＤＣ）を生成してサービスプロバイダ１００２に送信する。サービスプロバイダは、更新されたＩＤＣを自身の記憶手段に格納する。

【０４０２】

なお、上述のＩＤＣの有効期限の更新処理は、ＩＤＣの有効利用回数の更新、および個人識別認証局（ＩＤＡ）が設定するテンプレート有効期限の有効性消失時においても同様の手続きが適用可能である。

【０４０３】

次に、テンプレート情報の更新処理について説明する。テンプレートの更新は、既に個人識別認証局（ＩＤＡ）１００１に登録済みのテンプレート情報の有効期限を単に更新する場合と、既に登録済みのテンプレート情報を削除し、新たな指紋情報等の個人情報をユーザが入力して、その新たな個人情報に基づいてテンプレート情報を再生成する場合がある。前記の登録済みのテンプレート情報を用い、有効期限を再設定する場合は、前述のＩＤＣの有効期限、有効利用回数と同様の処理を実行すればよい。また、ユーザによってテンプレート情報の有効紀元が設定されている場合であっても、ユーザの了承を得ることで、個人識別認証局（ＩＤＡ）１００１において、テンプレート有効期限を再設定した個人識別証明書（ＩＤＣ）を生成することが可能である。

【０４０４】

しかし、既に登録済みのテンプレート情報を削除し、新たな指紋情報等の個人情報をユーザが入力して、その新たな個人情報に基づいてテンプレート情報を再生成する場合は、ユーザからの新たな個人識別情報の取得処理が必要となる。これらの処理について図８６、図８７を用いて説明する。

【０４０５】

図８６は、個人識別認証局（ＩＤＡ）１００１に登録済みのテンプレート情報の有効期限を個人識別認証局（ＩＤＡ）１００１がチェックし、有効期限切れであることをユーザに通知して更新を行なう場合の処理である。

【０４０６】

テンプレート情報の有効期限切れの通知を受領したユーザは、新たに指紋データ等の個人識別情報を、個人識別認証局（ＩＤＡ）１００１に送信する。なお、この処理は、個人の確認処理を再度実行することになるので、オフラインで行なうことが好ましい。ただし、個人確認が可能であればオンラインで実行してもよい。その際には、ユーザ側のデバイスと個人識別認証局（ＩＤＡ）１００１間での相互認証、通信データに対する署名付加、検証処理が実行される。

【０４０７】

個人識別認証局（ＩＤＡ）１００１では、個人確認が行われ、個人識別データをテンプレート情報として格納して新たなテンプレート有効期限を設定して、個人識別証明書（ＩＤＣ）を生成する。この有効期限は、ユーザ自身の設定要求に応じたデータとすることも可能である。個人識別認証局（ＩＤＡ）１００１によって新たにテンプレート有効期限の設定された個人識別証明書（ＩＤＣ）は、要求に応じてサービスプロバイダ等に送信され、個人認証が実行される。

【０４０８】

図８７は、ユーザ自身が自発的に個人識別認証局（ＩＤＡ）１００１に登録済みのテンプレート情報の更新を要求した場合の処理を説明する図である。

【０４０９】

テンプレート情報の更新要求を行なうユーザは、新たに指紋データ等の個人識別情報を、個人識別認証局（ＩＤＡ）１００１に送信する。なお、この処理は、個人の確認処理を再度実行することになるので、オフラインで行なうことが好ま

しい。ただし、個人確認が可能であればオンラインで実行してもよい。その際には、ユーザ側のデバイスと個人識別認証局（ＩＤＡ）１００１間での相互認証、通信データに対する署名付加、検証処理が実行される。

【０４１０】

個人識別認証局（ＩＤＡ）１００１では、個人確認が行われ、個人識別データをテンプレート情報として格納して新たなテンプレート有効期限を設定して、個人識別証明書（ＩＤＣ）を生成する。この有効期限は、ユーザ自身の設定要求に応じたデータとすることも可能である。さらに、個人識別認証局（ＩＤＡ）１００１では、例えばユーザの要求等、必要に応じて、現在有効期限内にある発行済みの個人識別証明書（ＩＤＣ）の無効化処理を実行する。ＩＤＣの無効化処理は、ＩＤＣ失効リストを既にＩＤＣを発行したサービスプロバイダ、ユーザデバイスに対して発行する処理として実行する。ＩＤＣ失効リストには失効したＩＤＣの識別データが記録されている。ＩＤＣ失効リストを受信したサービスプロバイダ、ユーザデバイスはＩＤＣを利用した個人認証を実行する際、ＩＤＣ失効リストに使用予定のＩＤＣ識別子が記録されているか否かをチェックし、記録されている場合は、そのＩＤＣの使用を中止する。必要であれば、新たに個人識別認証局（ＩＤＡ）１００１に対して更新ＩＤＣを要求して、その更新ＩＤＣを用いて個人認証を実行する。

【０４１１】

上述のように、個人認証処理実行エンティテイは、個人識別データであるテンプレートを格納した個人識別証明書に基づく個人認証処理の際に、証明書有効期限または証明書有効利用回数、またはテンプレート有効期限に基づき個人識別証明書の有効性確認処理を実行して、有効性が確認された場合にのみ、個人識別証明書に格納されたテンプレートと、ユーザ入力サンプリング情報との照合による個人認証を実行するので、個人識別認証局による個人識別証明書の有効性管理が可能となり、認証処理実行エンティテイまたは、被認証者の要求に応じて、個人識別認証局が個人識別証明書あるいはテンプレートの更新を実行する構成としたので、任意のタイミングでの個人識別証明書あるいはテンプレートの更新処理が可能となる。上述のような有効期限の設定により、例えば定期的なユーザ審査が

可能となり、また、個人識別証明書（ＩＤＣ）の発行対象者に対する有効性確認が容易となる。

【０４１２】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０４１３】

【発明の効果】

上述したように、本発明の個人識別証明書リンクシステム、情報処理装置、および情報処理方法においては、様々なデバイスにおいて容易に個人識別データであるテンプレートとユーザ入力サンプリング情報との照合による個人認証が可能となる。個人認証処理を実行する例えばサービスプロバイダ（ＳＰ）、ユーザデバイス（ＵＤ）は、第三者機関である個人識別認証局（ＩＤＡ）が生成した個人識別証明書（ＩＤＣ）からテンプレートを取得して個人認証を実行することが可能となる。個人識別証明書（ＩＤＣ）は、個人識別認証局（ＩＤＡ）がＩＤＣ発行要求者の個人確認処理を実行して、個人識別データとしてテンプレートを取得し生成するものであり、またサービスプロバイダ（ＳＰ）、ユーザデバイス（ＵＤ）に対する配布時には、ＩＤＡの署名がなされて配布される構成であるのでデータの正当性が保証され、正確な個人認証処理が可能となる。

【０４１４】

さらに、本発明の個人認証システム、個人認証方法、および情報処理装置においては、暗号処理鍵である公開鍵を格納し、認証局が生成する公開鍵証明書と、個人識別データであるテンプレートを格納し、個人識別認証局が生成する個人識別証明書との間で、証明書を関連づけたリンクを形成し、１つの証明書に基づいて他の関連証明書を特定可能としたことにより、例えば個人識別証明書に格納したテンプレートの暗号処理鍵の特定や、サービスプロバイダとの取り引き時に適用する個人識別証明書と公開鍵証明書との組を迅速に取得することが可能となり

、各種の処理において効率化が実現される。

【図面の簡単な説明】

【図１】

従来の指紋読み取り照合処理を実行する個人認証装置を示す図である。

【図２】

本発明の個人認証システムを利用し、かつ公開鍵証明書を用いた暗号化データ通信の概略を説明する図である。

【図３】

公開鍵証明書のデータ構成を説明する図である。

【図４】

公開鍵証明書のデータ構成を説明する図である。

【図５】

個人識別証明書のフォーマット例を示す図である。

【図６】

個人識別証明書のテンプレートの暗号化態様を説明する図である。

【図７】

個人識別証明書のテンプレートの暗号化に適用する鍵の種類および処理態様を説明する図である。

【図８】

個人識別証明書のテンプレートの暗号化態様を説明する図である。

【図９】

テンプレート登録、ＩＤＣ生成処理の流れを説明するフローおよびデータの流れを説明する図である。

【図１０】

テンプレート削除処理の流れを説明するフローおよびデータの流れを説明する図である。

【図１１】

テンプレート変更処理の流れを説明するフローおよびデータの流れを説明する図である。

【図１２】

テンプレート追加処理の流れを説明するフローおよびデータの流れを説明する図である。

【図１３】

テンプレート停止処理の流れを説明するフローおよびデータの流れを説明する図である。

【図１４】

テンプレート停止解除処理の流れを説明するフローおよびデータの流れを説明する図である。

【図１５】

ＩＤＣ配布処理の流れを説明するフローおよびデータの流れを説明する図である。

【図１６】

ＩＤＣ更新処理の流れを説明するフローおよびデータの流れを説明する図である。

【図１７】

ＩＤＣ削除処理の流れを説明するフローおよびデータの流れを説明する図である。

【図１８】

ＩＤＣ照会処理の流れを説明するフローおよびデータの流れを説明する図である。

【図１９】

公開鍵証明書（ＰＫＣ）を発行する認証局（ＣＡ）と、個人識別証明書（ＩＤＣ）を発行する個人識別認証局（ＩＤＡ）と、証明書を利用するデバイスの構成例を示す図である。

【図２０】

公開鍵証明書（ＰＫＣ）を発行する認証局（ＣＡ）と、個人識別証明書（ＩＤＣ）を発行する個人識別認証局（ＩＤＡ）と、証明書を利用するデバイスの構成例を示す図である。

【図２１】

ユーザデバイス、サービスプロバイダ（ＳＰ）、個人識別認証局（ＩＤＡ）の各システムにおける照合処理の実行形態を説明する図である。

【図２２】

ユーザデバイスにおいて照合処理を実行する形態を説明する図である。

【図２３】

サービスプロバイダ（ＳＰ）において照合処理を実行する形態を説明する図である。

【図２４】

ＩＤＣとＰＫＣを格納したユーザデバイスにおける照合処理を説明する図である。

【図２５】

ＩＣカード等の個人端末に格納された個人識別証明書（ＩＤＣ）を共有型ユーザデバイスへ送信して照合処理を実行する構成について説明する図である。

【図２６】

ＩＣカード等の個人端末に格納された個人識別証明書（ＩＤＣ）を復号した後、共有型ユーザデバイスへ送信して照合処理を実行する構成について説明する図である。

【図２７】

ＩＣカード等の個人端末に格納された個人識別証明書（ＩＤＣ）を用いて個人端末側で照合処理を実行して、その結果のみを共有型ユーザデバイスへ送信する構成について説明する図である。

【図２８】

個人識別証明書（ＩＤＣ）のテンプレート情報がサービスプロバイダ（ＳＰ）の公開鍵で暗号化されている場合の処理を説明する図である。

【図２９】

ユーザデバイスに格納された個人識別証明書（ＩＤＣ）をサービスプロバイダ（ＳＰ）へ送信して照合処理を実行する構成について説明する図である。

【図３０】

ユーザデバイスに格納された個人識別証明書（ＩＤＣ）を復号した後、サービスプロバイダ（ＳＰ）へ送信して照合処理を実行する構成について説明する図である。

【図３１】

ユーザデバイスに格納された個人識別証明書（ＩＤＣ）を用いてユーザデバイス側で照合処理を実行して、その結果のみをサービスプロバイダ（ＳＰ）へ送信する構成について説明する図である。

【図３２】

コンテンツ取り引きにおいて流通するコンテンツを含むセキュア・コンテナ（Ｓｅｃｕｒｅ　Ｃｏｎｔａｉｎｅｒ）の構成を示す図である。

【図３３】

個人識別証明書（ＩＤＣ）のリスト構成を示す図である。

【図３４】

販売条件（ＵＣＰ）の具体的構成例を示す図である。

【図３５】

利用権データの構成例を示す図である。

【図３６】

セキュアコンテナに含まれる価格情報のデータ構成例を示す図である。

【図３７】

セキュアコンテンナを利用したコンテンツの配信処理形態を示す図である。

【図３８】

使用制御情報（ＵＣＳ：Usage Control Status）の例を示す図である。

【図３９】

コンテンツを格納したセキュアコンテナをサービスプロバイダからユーザデバイスに配信する際の個人識別証明書（ＩＤＣ）の利用を説明する図である。

【図４０】

セキュアコンテナをサービスプロバイダから受領し、ユーザデバイスにおいて個人認証処理を実行して、正当なユーザにのみコンテンツ利用を可能とした処理フローを示す図である。

【図４１】

サービスプロバイダにおいて個人認証処理を実行して、正当なユーザにのみセキュアコンテナを配信する処理フローを示す図である。

【図４２】

セキュアコンテンナを利用したコンテンツのユーザ間の配信処理形態を示す図である。

【図４３】

セキュアコンテンナを利用したコンテンツのユーザ間の配信処理、ユーザの個人認証の異なる形態を示す図である。

【図４４】

セキュアコンテナをユーザデバイスＡから受領し、ユーザデバイスＢにおいて個人認証処理を実行して、正当なユーザにのみコンテンツ利用を可能とした処理フローを示す図である。

【図４５】

コンテンツを配信する前に配信元において個人認証処理を実行して、正当なユーザにのみセキュアコンテナを配信する処理フローを示す図である。

【図４６】

ユーザデバイス間でのセキュアコンテナの転送処理を実行するユーザデバイス構成を中心としたブロック図である。

【図４７】

個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）とのリンク態様のそれぞれについて示す図である。

【図４８】

個人識別証明書（ＩＤＣ）と公開鍵証明書（ＰＫＣ）とのリンク態様のそれぞれについて示す図である。

【図４９】

リンクする公開鍵証明書（ＰＫＣ）の個人識別証明書（ＩＤＣ）に対する格納態様を説明する図である。

【図５０】

証明書の識別番号を他の証明書（ＩＤＣ）に格納する構成例を示す図である。

【図５１】

リンク管理用データを用いた管理構成例を示す図である。

【図５２】

リンク管理用データを用いた管理構成例を示す図である。

【図５３】

個人認証を実行し、かつコンテンツ再生可能なユーザデバイスの構成を示す図である。

【図５４】

コンテンツダウンロード処理におけるデータの流れを説明する図である。

【図５５】

コンテンツダウンロード処理の流れを説明する詳細処理フロー図である。

【図５６】

コンテンツダウンロード処理の流れを説明する詳細処理フロー図である。

【図５７】

コンテンツダウンロード処理の流れを説明する詳細処理フロー図である。

【図５８】

ユーザ登録、ユーザ登録抹消、サービス契約処理におけるデータの流れを説明する図である。

【図５９】

ユーザ登録、ユーザ登録抹消、サービス契約処理を説明する詳細処理フロー図である。

【図６０】

ユーザ登録、ユーザ登録抹消、サービス契約処理を説明する詳細処理フロー図である。

【図６１】

ユーザ登録、ユーザ登録抹消、サービス契約処理を説明する詳細処理フロー図である。

【図６２】

デバイスに格納する個人識別証明書（ＩＤＣ）の要求処理におけるデータの流れを説明する図である。

【図６３】

デバイスに格納する個人識別証明書（ＩＤＣ）の要求処理の流れを説明する詳細処理フロー図である。

【図６４】

デバイスに格納する個人識別証明書（ＩＤＣ）の要求処理の流れを説明する詳細処理フロー図である。

【図６５】

デバイスに格納する個人識別証明書（ＩＤＣ）の要求処理の流れを説明する詳細処理フロー図である。

【図６６】

ワンタイムＰＫＣの発行手順を説明する図である。

【図６７】

ワンタイムＰＫＣの発行手順を示すフロー図である。

【図６８】

照合証明書の第１の利用形態を説明する図である。

【図６９】

照合証明書の利用処理フローを示す図である。

【図７０】

照合証明書の第２の利用形態を説明する図である。

【図７１】

照合証明書のフォーマット例を示す図である。

【図７２】

個人識別認証局（ＩＤＡ）に登録済みの個人識別証明書（ＩＤＣ）を利用して個人認証を行ない、さらに、個人認証処理に基づいてコンテンツ配信を受ける処理を説明する図である。

【図７３】

ＩＤＣを利用した個人認証、ＰＫＣを利用した相互認証を実行してコンテンツ

の配信サービスを実行する処理を示すフロー図である。

【図７４】

ＩＤＣを利用した個人認証、ＰＫＣを利用した相互認証を実行してコンテンツの配信サービスを実行する処理を示すフロー図である。

【図７５】

ＩＤＣを利用した個人認証、ＰＫＣを利用した相互認証を実行してコンテンツの配信サービスを実行する処理を示すフロー図である。

【図７６】

ユーザＩＤＣと、デバイスＰＫＣを用い、個人識別認証局（ＩＤＡ）に登録済みのＩＤＣを利用して個人認証を行ない、デバイスＰＫＣに基づいてコンテンツ配信を受ける処理を説明する図である。

【図７７】

ユーザＩＤＣと、デバイスＰＫＣを用い、個人識別認証局（ＩＤＡ）に登録済みのＩＤＣを利用して個人認証を行ない、デバイスＰＫＣに基づいてコンテンツ配信を受ける処理フローを示す図である。

【図７８】

ユーザＩＤＣと、デバイスＰＫＣを用い、個人識別認証局（ＩＤＡ）に登録済みのＩＤＣを利用して個人認証を行ない、デバイスＰＫＣに基づいてコンテンツ配信を受ける処理フローを示す図である。

【図７９】

個人識別証明書（ＩＤＣ）の有効情報（有効期限および有効利用回数）と、ＩＤＣに格納したテンプレート情報の有効期限とを設定した個人識別証明書構成を示す図である。

【図８０】

個人識別証明書（ＩＤＣ）に格納された［利用有効期限または有効回数］、およびテンプレート情報の［テンプレート有効期限］の管理構成を説明する図である。

【図８１】

ＩＤＣ有効期限、テンプレート有効期限の管理構成を説明する図である。

【図８２】

ＩＤＣ有効利用回数、テンプレート有効期限の管理構成を説明する図である。

【図８３】

個人識別証明書（ＩＤＣ）の［利用有効期限または有効回数］、および［テンプレート有効期限］に基づいたＩＤＣ利用制御処理ヲ説明するフロー図である。

【図８４】

個人識別証明書（ＩＤＣ）の利用時に、ＩＤＣの［利用有効期限］の期限切れが判明した場合のＩＤＣ更新処理を説明する図である。

【図８５】

定期的な個人識別証明書（ＩＤＣ）の期限チェックを実行して、ＩＤＣの［利用有効期限］の期限切れが判明した場合のＩＤＣ更新処理について説明する図である。

【図８６】

個人識別認証局（ＩＤＡ）に登録済みのテンプレート情報の有効期限をＩＤＡがチェックし、有効期限切れであることをユーザに通知して更新を行なう場合の処理を説明する図である。

【図８７】

ユーザ自身が自発的に個人識別認証局（ＩＤＡ）に登録済みのテンプレート情報の更新を要求した場合の処理を説明する図である。

【符号の説明】

１０　個人認証装置

１１　個人情報取得部

１２　情報変換部

１３　比較部

１４　セキュアメモリ

１５　制御部

１６　通信部

２０　パーソナルコンピュータ

２０１　個人識別認証局（ＩＤＡ）

２０２　認証局（ＣＡ）

２０３，２０４　サービスプロバイダ（ＳＰ）

２０５，２０６　ユーザデバイス

３００　サービスプロバイダ（ＳＰ）

３１０　サンプリング情報処理部

３１１　制御部

３１２　通信部

３１３　情報変換部

３１４　個人情報取得部

３１５　公開鍵証明書

３２０　個人識別認証局（ＩＤＡ）

３２１　比較部

３２２　記憶手段

３３０　認証局（ＣＡ）

４００　サービスプロバイダ（ＳＰ）

４１０　照合システム

４１１　通信部

４１２　制御部

４１３　メモリ

４１４　個人識別証明書検証部

４１５　テンプレート復号化部

４１６　比較部

４１７　情報変換部

４１８　個人情報取得部

４１９　暗号処理部

４２０　個人識別認証局

４２１　個人識別証明書発行部

４２２　記憶手段

４３０　認証局

４５０　ＩＣカード
５００　ユーザデバイス
５０１　コンテンツ再生機構部
５０２　コンテンツデータ蓄積部
５０３　個人識別装置
５０４　ネットワーク接続部
５０５　公開鍵暗号処理部
５０６　選択機能部
５０７　入出力機能部
７００　セキュアコンテナ
７０１　コンテンツ
７０２　価格情報
７０３　販売情報（ＵＣＰ）
７０４　電子署名
７１１　ＩＤＣ識別子リスト
７１２　ＵＣＰ世代管理情報
７１３　二次配信可能回数
７２１　ＩＤＣ識別子リスト
７３１　ＩＤＣ識別子リスト
７３２　ＵＣＳ世代管理情報
７３３　ＵＣＳ二次配信可能回数
８０１　コンテンツプロバイダ
８０２　サービスプロバイダ
８０３，８０５　ユーザデバイス
８０４　クリアリングセンタ
８１０　ユーザデバイス
８２０　ユーザ
８３０　個人識別認証局（ＩＤＡ）
８４０　サービスプロバイダ

９１０　個人識別認証局（ＩＤＡ）

９２０　ユーザデバイス１

９３０　ユーザデバイス２

９４０，９４５　ユーザ

９５０　ユーザデバイス１

９５５，９６５　個人識別証明書

９６０　ユーザデバイス２

９７０　個人識別認証局（ＩＤＡ）

９９０　セキュアコンテナ

９９２　ＩＤＣ識別子リスト

１００１　個人識別認証局（ＩＤＡ）

１００２　サービスプロバイダ

１００３　ユーザ端末

１００４　ＩＤＣ利用有効期限／有効回数情報

１００５　テンプレート有効期限情報

１００６　ＩＤＡ署名

１０１４　ＩＤＣ利用有効期限

１０１５　テンプレート有効期限情報

１０１６　ＩＤＡ署名

１０１７　ＩＤＣ利用有効回数

１０１８　ＳＡＭ署名

１０１９　ＩＤＣ利用回数ＳＡＭ内設定情報

１０２０　ＳＡＭ（Secure Application Module）

１８１０　サービスプロバイダ

１８１１　制御部

１８１２　コンテンツデータベース

１８１３　ユーザ情報データベース

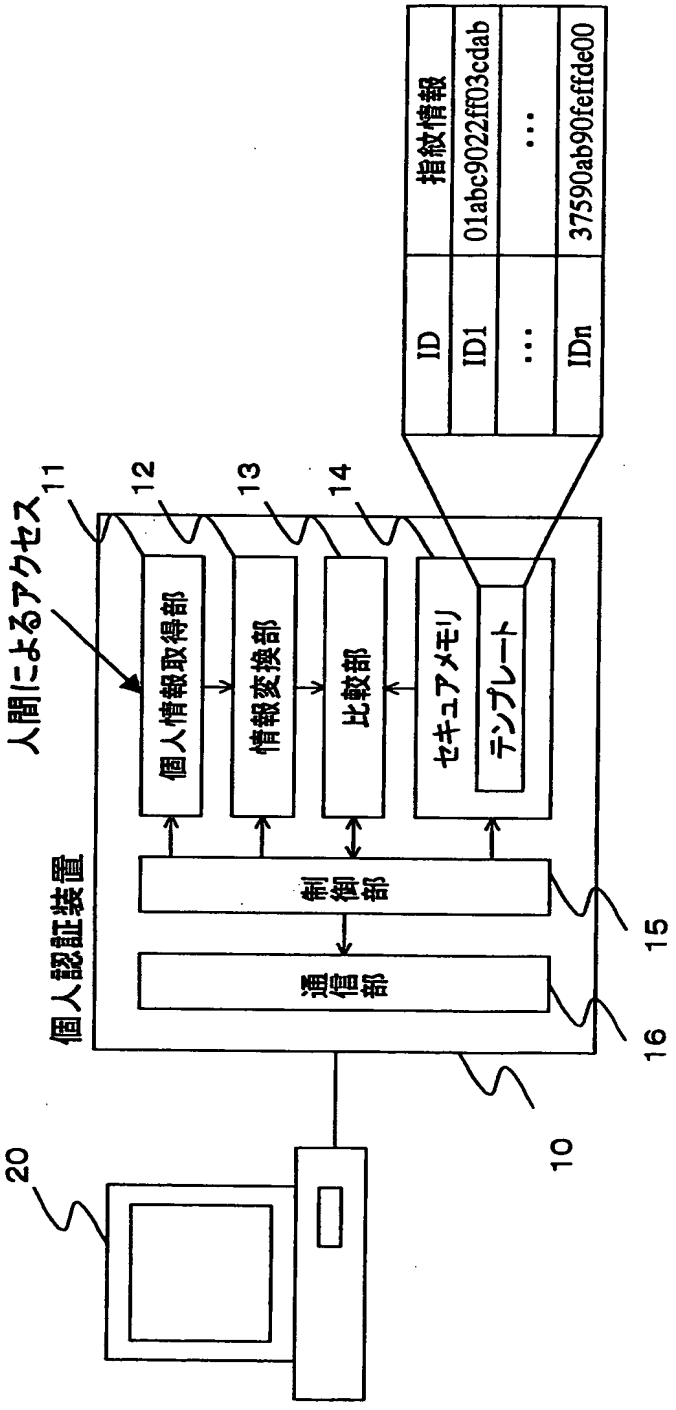
１８１４　暗号処理部

１８１５　通信部

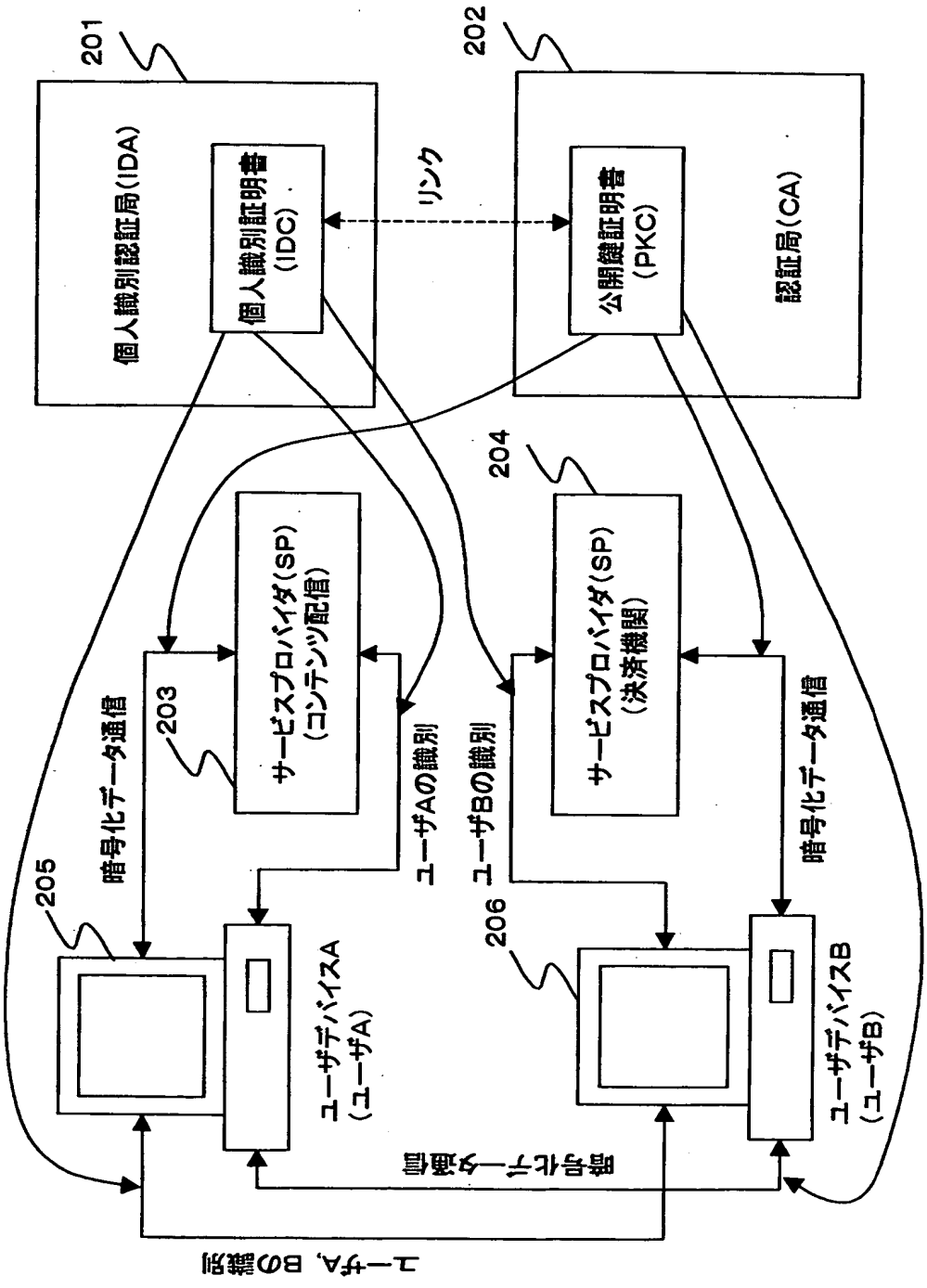
１８１６　個人識別装置
１８２０　ユーザデバイスＡ
１８３０　ユーザデバイスＢ
１８２１，１８３１　制御部
１８２２，１８３２　暗号処理部
１８２４，１８３４　メモリ
１８２５，１８３５　記憶部
１８２６，１８３６　データ再生部
１８２７，１８３７　通信部
１８２８，１８３８　電子マネー
１８２９，１８３９　個人識別装置
１８４０　クリアリングセンタ
１８４１　制御部
１８４２　データベース
１８４４　暗号処理部
１８４５　通信部
１８４６　個人識別装置

【書類名】　　図面

【図１】


ID
指紋情報
ID1
01abc9022ff03cdab
…
…
IDn
37590ab90feffde00
人間によるアクセス
11
12
13
14
個人情報取得部
情報変換部
比較部
セキュアメモリ
テンプレート
制御部
通信部
15
16
個人認証装置
10
20

【図２】


201
個人識別認証局(IDA)
個人識別証明書
(IDC)
リンク
202
公開鍵証明書
(PKC)
認証局(CA)
204
サービスプロバイダ(SP)
(決済機関)
サービスプロバイダ(SP)
(コンテンツ配信)
203
暗号化データ通信
ユーザAの識別
ユーザBの識別
暗号化データ通信
205
206
ユーザデバイスA
(ユーザA)
ユーザデバイスB
(ユーザB)
暗号化データ通信
ユーザA, Bの識別

【図３】

証明書フォーマット例 (X.509 V3に準拠)

項目	説明	本IAにおける設定
Version1		
version	証明書のフォーマットのバージョン	V3
serial Number	IA によってつけられる証明書のSerial No.	シーケンシャルなシリアルナンバー
signature.algorithm Identifier algorithm parameters	証明書の署名アルゴリズム、及びそのパラメータ	楕円曲線暗号/RSA 楕円の場合パラメータ RSAの場合:鍵長
issuer	IA 名 (Distinguished Name形式)	本ＩＡの名称
validity notBefore notAfter	証明書の有効期限 開始日時 終了日時	
subject	user を識別する名前	ユーザ機器ID またはサービス主体のID
subject Public Key Info algorithm subject Public key	user の公開鍵情報 鍵のアルゴリズム 鍵	楕円曲線/RSA user の公開鍵
Version3		
authority Key Identifier key Identifier authority Cert Issuer authority Cert Serial Number	IA の署名確認用の鍵識別 鍵識別番号 (8 進数) IA 名(General Name形式) 認証番号	
subject key Identifier	複数の鍵の証明をする場合	利用しない
key usage (0)digital Signature (1)non Repudiation (2)key Encipherment (3)data Encipherment (4)key Agreement (5)key CertSign (6)cRL Sign	鍵の使用目的を指定 (0)デジタル署名用 (1)否認防止用 (2)鍵の暗号化用 (3)メッセージの暗号化用 (4)共通鍵配送用 (5)認証の署名確認用 (6)失効リストの署名確認用	0,1,4,6 を利用
private Key Usage Period notBefore notAfter	user に格納されている秘密鍵の有効期限。	証明書の有効期限 =公開鍵の有効期限 =秘密鍵の有効期限 (default)

【図４】

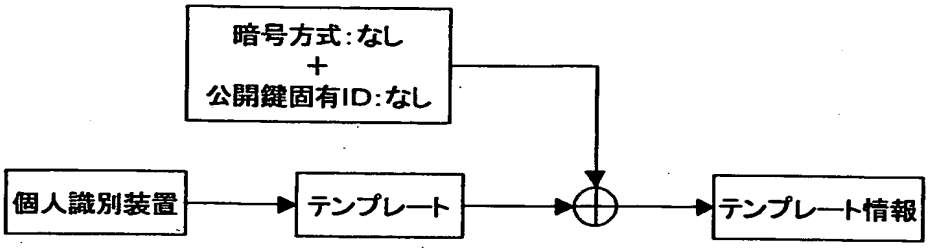
Certificate Policy policy Identifier policy Qualifiers	認証局の証明書発行ポリシー ポリシーID(ISO/IEC9834-1に準拠) 認証基準	
policy Mappings issuer Domain Policy subject Domain Policy	CA を認証する場合にのみ必要。発行認証局のポリシーと被認証ポリシーのマッピングを規定	default = なし
supported Algorithms algorithm Identifier intended Usage intended Certificate Policies	ディレクトリ (X.500) のアトリビュートを定義。コミュニケーションの相手がディレクトリ情報を利用する場合に、事前にそのアトリビュートを知らせるのに用いる。	default = なし
subject Alt Name	user の別名 (GN 形式) 。	利用しない
issuer Alt Name	項目は入れておく(default = なし)	default = なし
subject Directory Attributes	user の任意の属性。	利用しない
basic Constraints	証明対象の公開鍵が認証	
cA path Len Constraint	局の署名用か、user のものかを区別	default = user用
name Constraints permitted Subtrees base minimum	被認証者が認証局である場合 (CA 認証) にのみ使用。	default = なし
maximum excluded Subtrees		
policy Constraints requireExplicitPolicy inhibitPolicyMapping	認証パスの残りに対する明確な認証ポリシー ID、禁止ポリシーマップを要求する制限を記述	
CRL Distribution Points	user が証明書を利用する際に、証明書が失効していないかどうかを確認す	証明書を登録したところへのポインタ。失効リストは、発行元で管理
	るための失効リストの参	
	照ポイントを記述。	
署名	発行者の署名	

【図５】

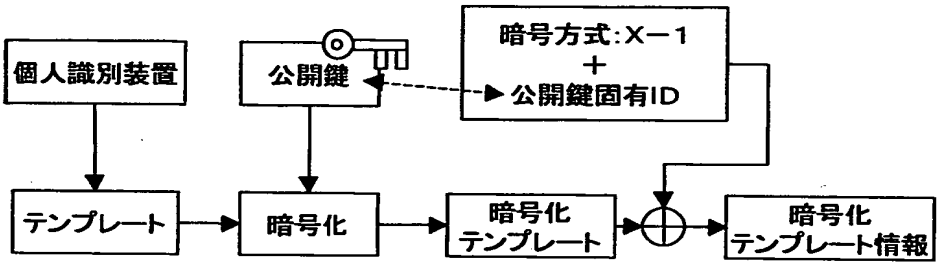
	項目	説明
必須項目	Version	バージョン
	SerialNumber	識別番号
	signaturealgorithmIdentifier algorithm parameters	署名方式 アルゴリズム パラメータ
	Issuer	個人識別認証局名(Distinguished Name形式)
	Validity notBefore notAfter	有効期限 ・開始日時 ・終了日時
	Subject	被認証者名(DN形式)
	subjectTemplateInfo encryptType encryptUniqueID encryption Algorithm parameter validity subjectTemplate Source subjectTemplate	テンプレート情報 ・暗号方式 ・暗号化するために使用した公開鍵証明書の固有IDまたは認証番号 ・アルゴリズム ・パラメータ ・有効期限（開始日時：終了日時） ・テンプレートの種別 ・テンプレート
拡張項目	SubjectPKCinfo subjectPKCserialNumber subjectPKCUniqueID	被認証者の公開鍵証明書情報 ・被認証者の公開鍵証明書の認証番号 ・被認証者の公開鍵証明書の被認証者固有ID
	IssuerUniqueID	個人識別認証局の固有ID
	SubjectUniqueID	被認証者の固有ID
	PublicKey Certificate	公開鍵証明書
	Issuer Alt Name	個人識別認証局の別名
	subjectDirectoryAttributes	個人情報（必要に応じて暗号化） 本人確認のための情報 年齢、性別、ｅｔｃ
	Valid Count	有効回数
	Control Table Link Info Ctl Tbl Location Ctl Tbl Unique ID	組情報へのリンク情報 ・組情報管理テーブルのある場所(URL,IP address等) ・組情報識別番号
必須	IDASignature	IDAの署名

【図６】

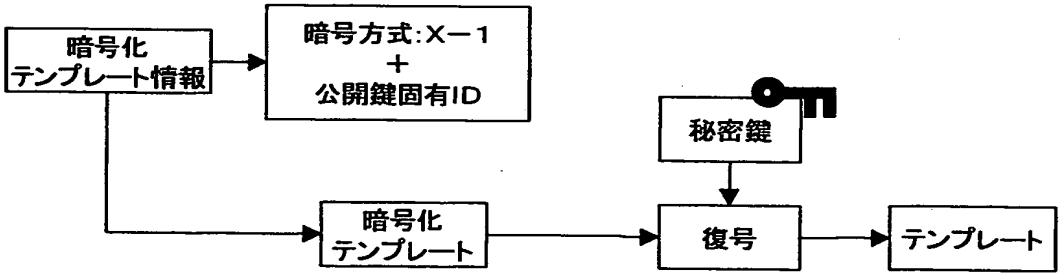
(a)非暗号化



(b－1)公開鍵のみを使用した暗号化



(b－2)秘密鍵のみを使用した復号化

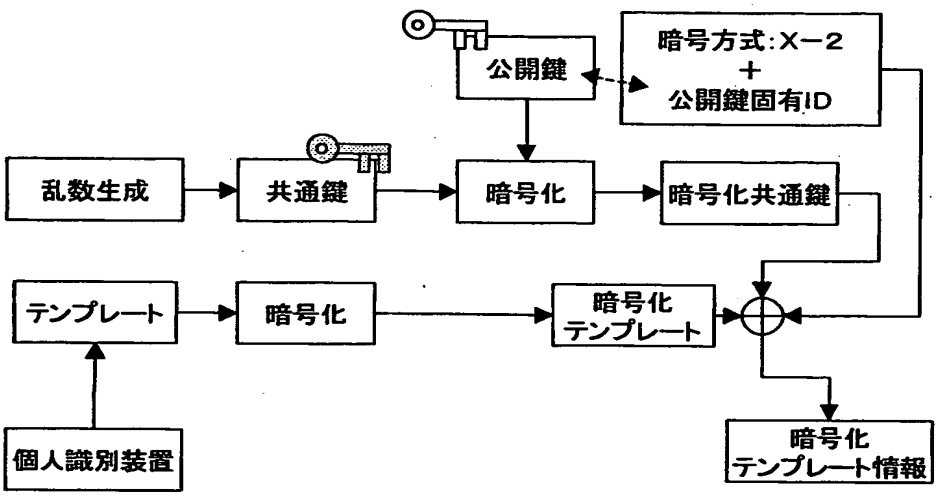


【図７】

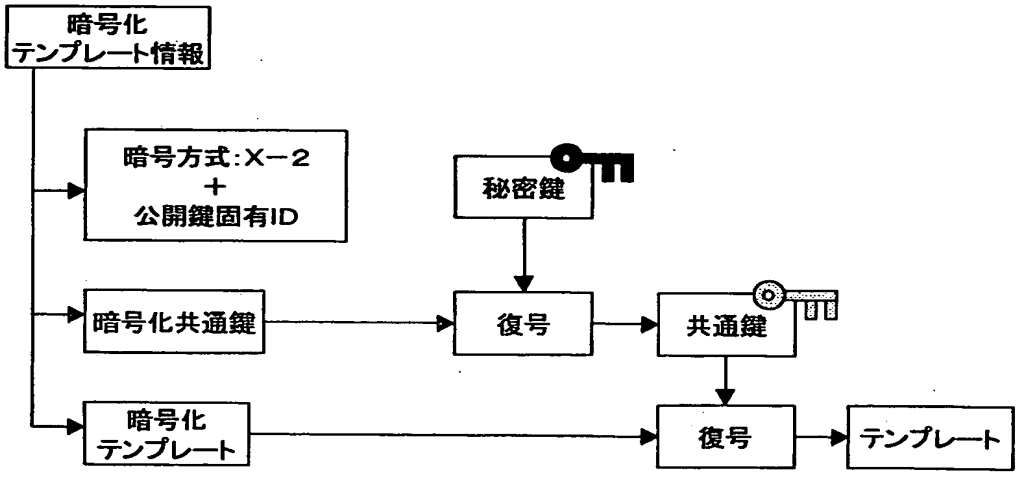
テンプレート暗号化に用いる公開鍵	テンプレート情報格納IDCの使用例
ユーザまたはユーザデバイスの公開鍵	ユーザデバイス（例えばPC）の使用許可を付与した特定ユーザの識別を、各ユーザ毎の個人識別証明書（IDC）を用いて識別処理を行なう場合等
サービスプロバイダの公開鍵	サービスプロバイダにおいて、特定ユーザ、例えばサービスを提供するユーザを識別するために、各ユーザの個人識別証明書（IDC）を用いて個人識別を行なう場合等
個人識別認証局の公開鍵	様々な端末間でのデータ送受信における、データ送受信者において、個人識別認証局（IDA）発行の個人識別証明書（IDC）を用いて個人識別処理を行なう場合等、

【図８】

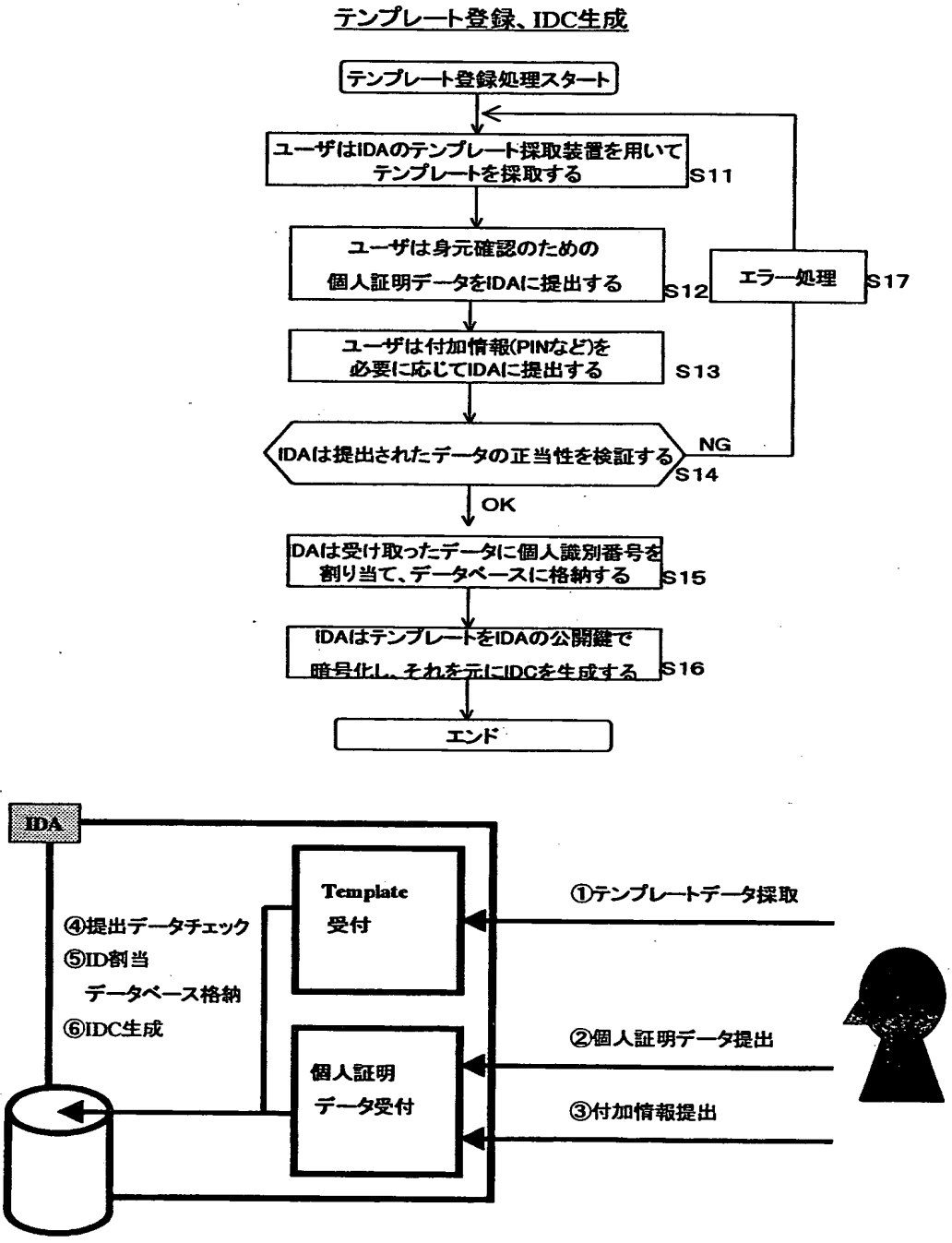
（ｃ－１）共通鍵と公開鍵を使用した暗号化



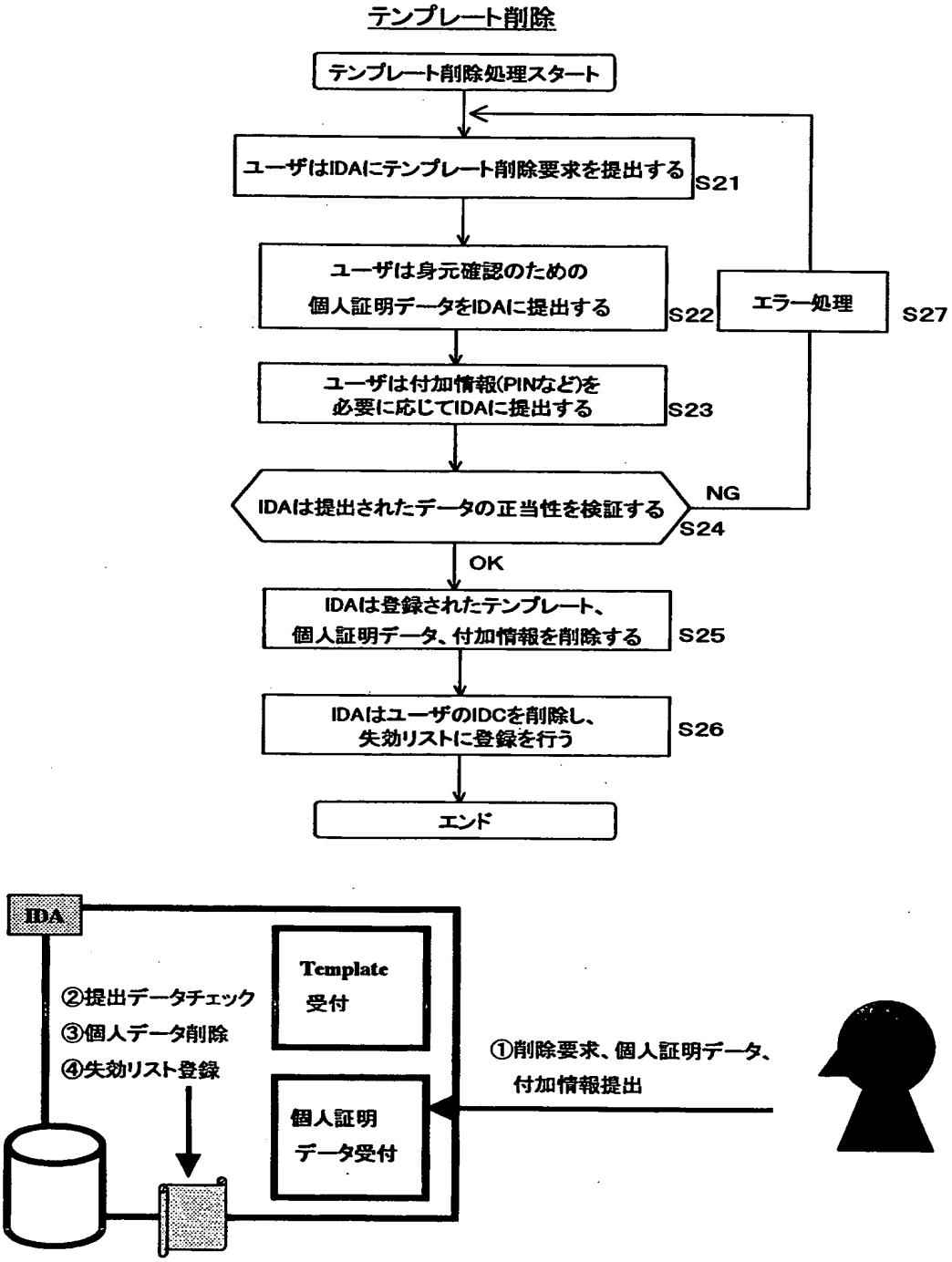
（ｃ－２）共通鍵と秘密鍵を使用した復号化



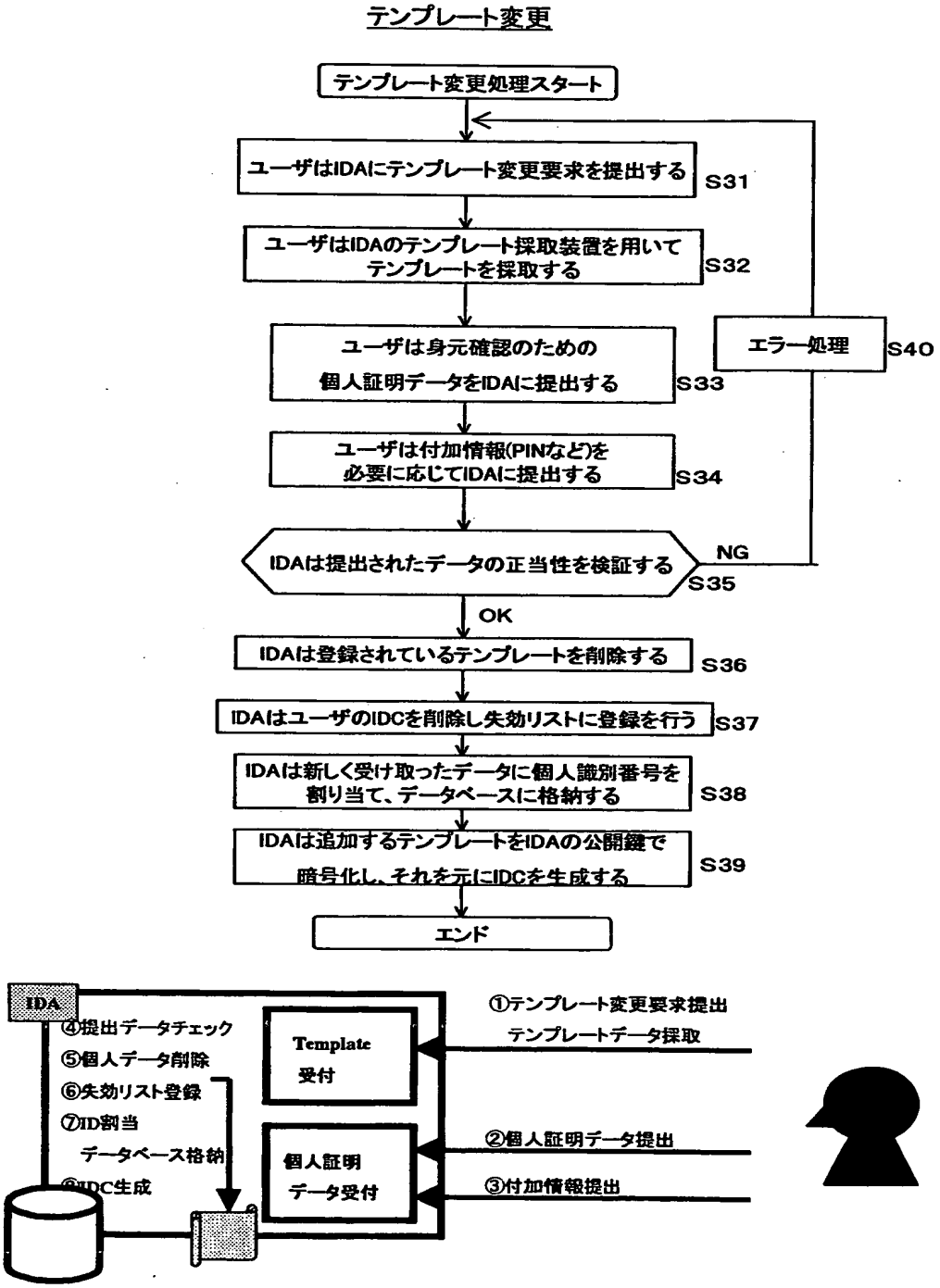
【図９】


テンプレート登録、IDC生成
テンプレート登録処理スタート
ユーザはIDAのテンプレート採取装置を用いて
テンプレートを採取する
S11
ユーザは身元確認のための
個人証明データをIDAに提出する
S12
エラー処理
S17
ユーザは付加情報(PINなど)を
必要に応じてIDAに提出する
S13
IDAは提出されたデータの正当性を検証する
NG
S14
OK
IDAは受け取ったデータに個人識別番号を
割り当て、データベースに格納する
S15
IDAはテンプレートをIDAの公開鍵で
暗号化し、それを元にIDCを生成する
S16
エンド
IDA
Template
受付
個人証明
データ受付
④提出データチェック
⑤ID割当
データベース格納
⑥IDC生成
①テンプレートデータ採取
②個人証明データ提出
③付加情報提出

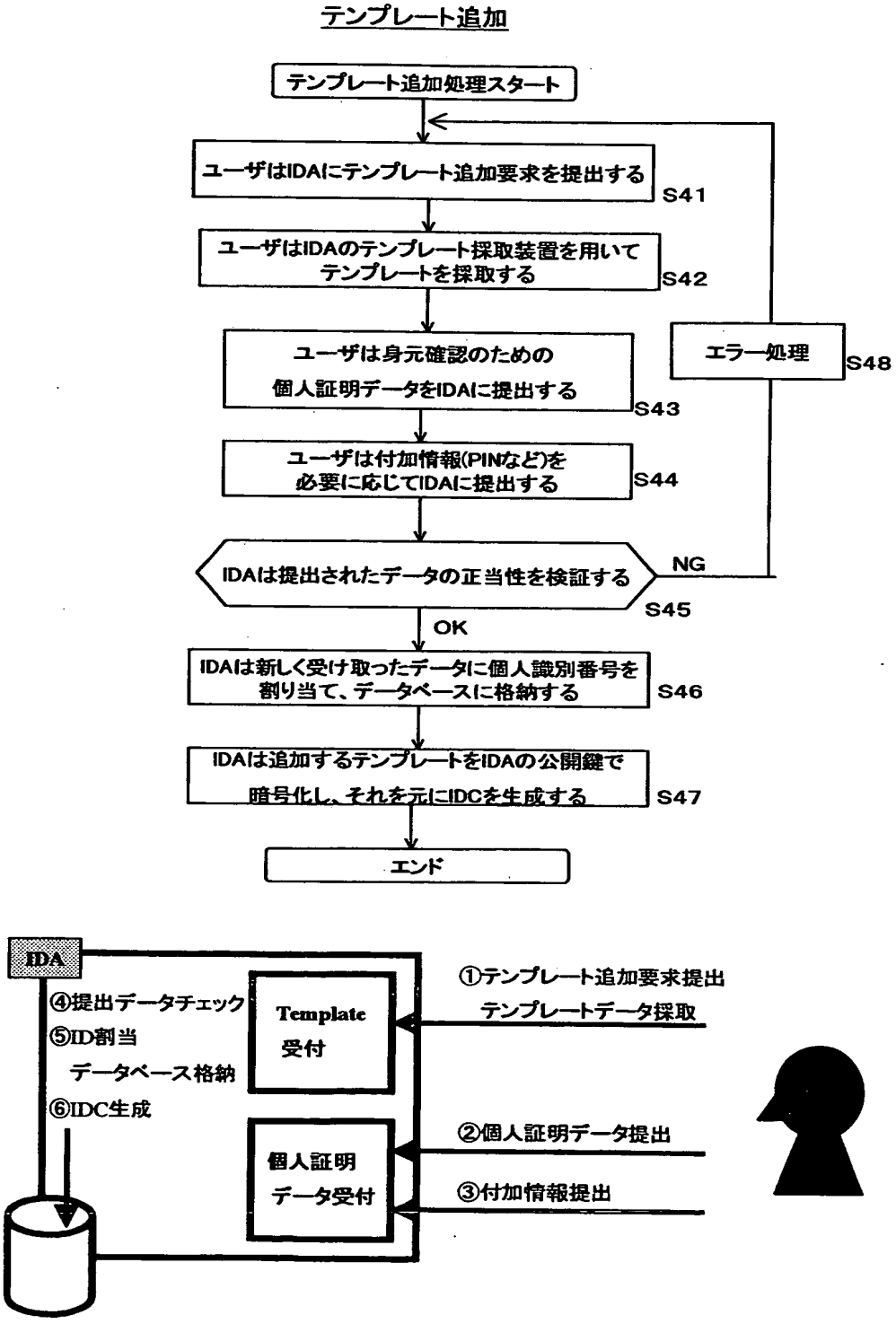
【図１０】


テンプレート削除
テンプレート削除処理スタート
ユーザはIDAにテンプレート削除要求を提出する
S21
ユーザは身元確認のための
個人証明データをIDAに提出する
S22
エラー処理
S27
ユーザは付加情報(PINなど)を
必要に応じてIDAに提出する
S23
IDAは提出されたデータの正当性を検証する
NG
S24
OK
IDAは登録されたテンプレート、
個人証明データ、付加情報を削除する
S25
IDAはユーザのIDCを削除し、
失効リストに登録を行う
S26
エンド
IDA
Template
受付
②提出データチェック
③個人データ削除
④失効リスト登録
個人証明
データ受付
①削除要求、個人証明データ、
付加情報提出

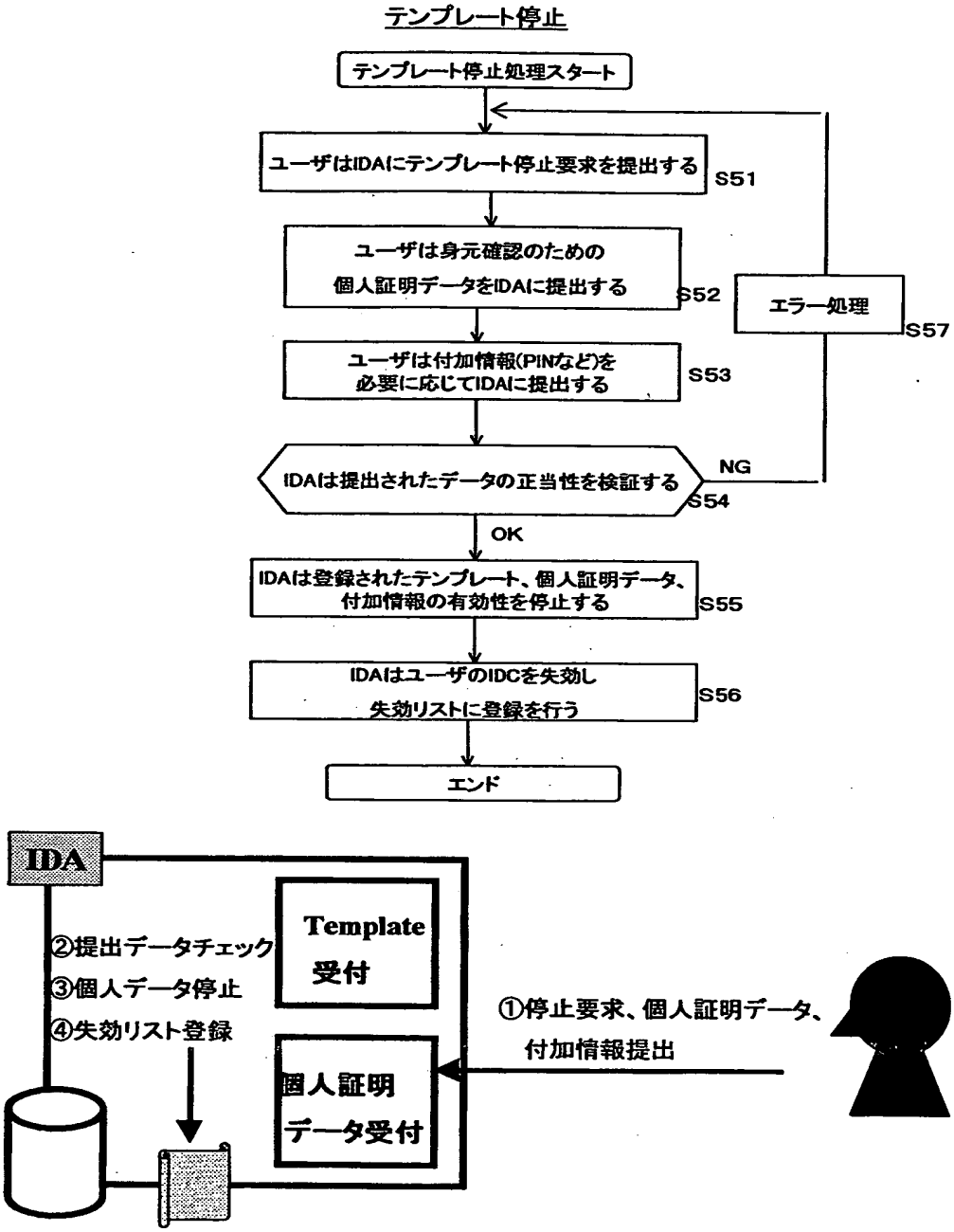
【図１１】


テンプレート変更
テンプレート変更処理スタート
ユーザはIDAにテンプレート変更要求を提出する
S31
ユーザはIDAのテンプレート採取装置を用いて
テンプレートを採取する
S32
ユーザは身元確認のための
個人証明データをIDAに提出する
S33
エラー処理
S40
ユーザは付加情報(PINなど)を
必要に応じてIDAに提出する
S34
IDAは提出されたデータの正当性を検証する
NG
S35
OK
IDAは登録されているテンプレートを削除する
S36
IDAはユーザのIDCを削除し失効リストに登録を行う
S37
IDAは新しく受け取ったデータに個人識別番号を
割り当て、データベースに格納する
S38
IDAは追加するテンプレートをIDAの公開鍵で
暗号化し、それを元にIDCを生成する
S39
エンド
IDA
④提出データチェック
⑤個人データ削除
⑥失効リスト登録
⑦ID割当
データベース格納
⑧IDC生成
Template
受付
個人証明
データ受付
①テンプレート変更要求提出
テンプレートデータ採取
②個人証明データ提出
③付加情報提出

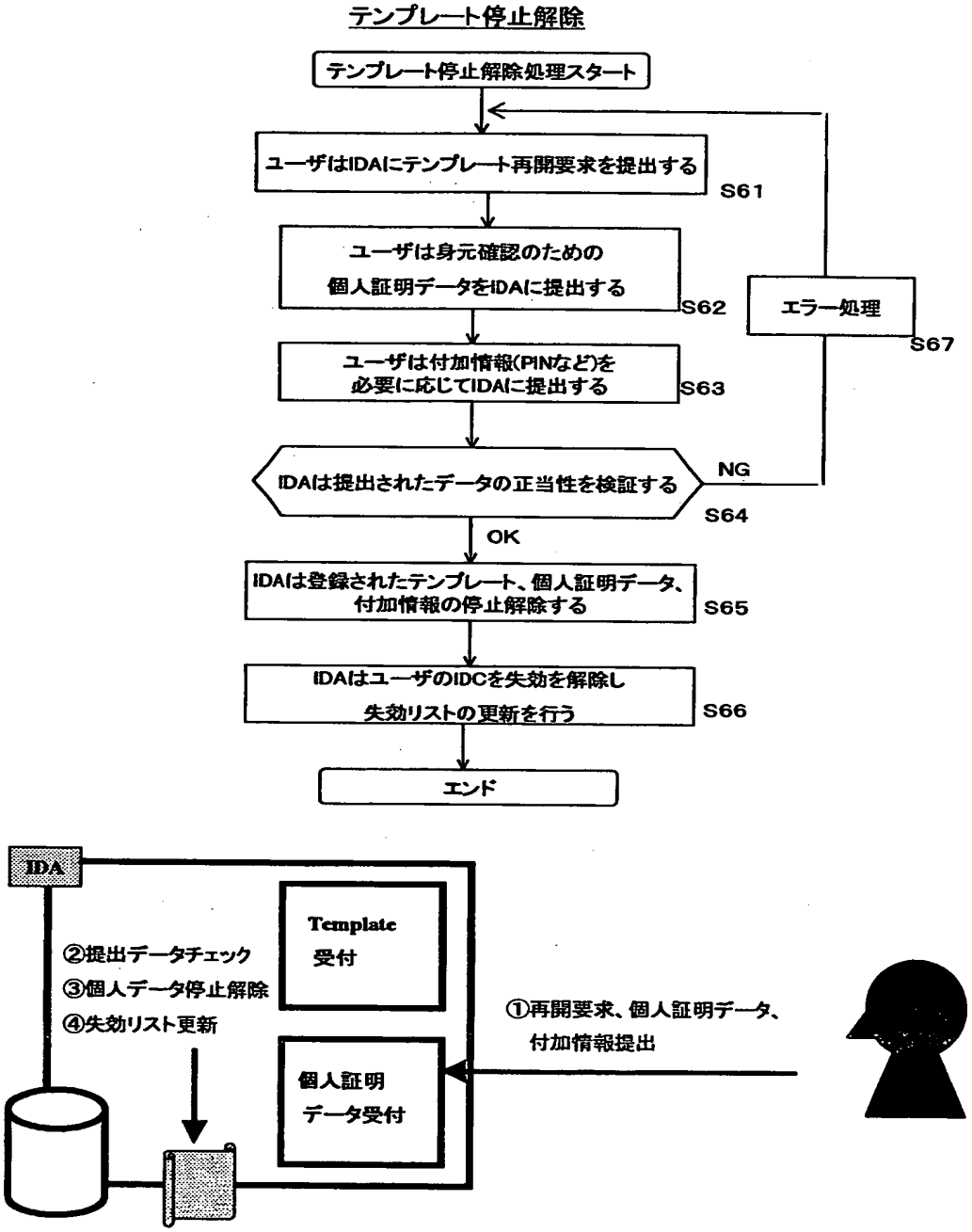
【図１２】


テンプレート追加
テンプレート追加処理スタート
ユーザはIDAにテンプレート追加要求を提出する
S41
ユーザはIDAのテンプレート採取装置を用いて
テンプレートを採取する
S42
ユーザは身元確認のための
個人証明データをIDAに提出する
S43
ユーザは付加情報(PINなど)を
必要に応じてIDAに提出する
S44
IDAは提出されたデータの正当性を検証する
S45
NG
エラー処理
S48
OK
IDAは新しく受け取ったデータに個人識別番号を
割り当て、データベースに格納する
S46
IDAは追加するテンプレートをIDAの公開鍵で
暗号化し、それを元にIDCを生成する
S47
エンド
IDA
④提出データチェック
⑤ID割当
データベース格納
⑥IDC生成
Template
受付
個人証明
データ受付
①テンプレート追加要求提出
テンプレートデータ採取
②個人証明データ提出
③付加情報提出

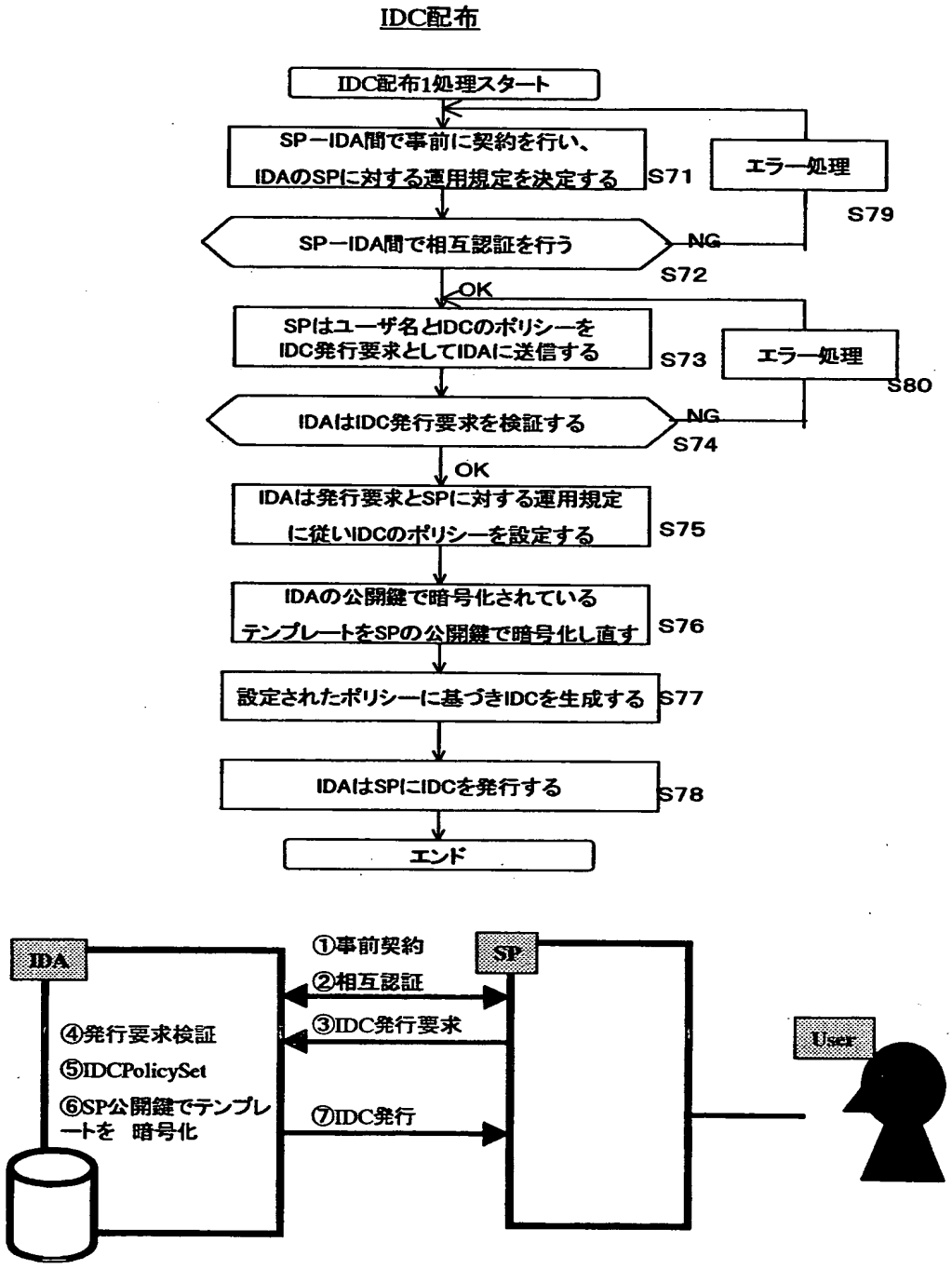
【図１３】


テンプレート停止
テンプレート停止処理スタート
ユーザはIDAにテンプレート停止要求を提出する
S51
ユーザは身元確認のための
個人証明データをIDAに提出する
S52
エラー処理
S57
ユーザは付加情報(PINなど)を
必要に応じてIDAに提出する
S53
IDAは提出されたデータの正当性を検証する
NG
S54
OK
IDAは登録されたテンプレート、個人証明データ、
付加情報の有効性を停止する
S55
IDAはユーザのIDCを失効し
失効リストに登録を行う
S56
エンド
IDA
②提出データチェック
③個人データ停止
④失効リスト登録
Template
受付
個人証明
データ受付
①停止要求、個人証明データ、
付加情報提出

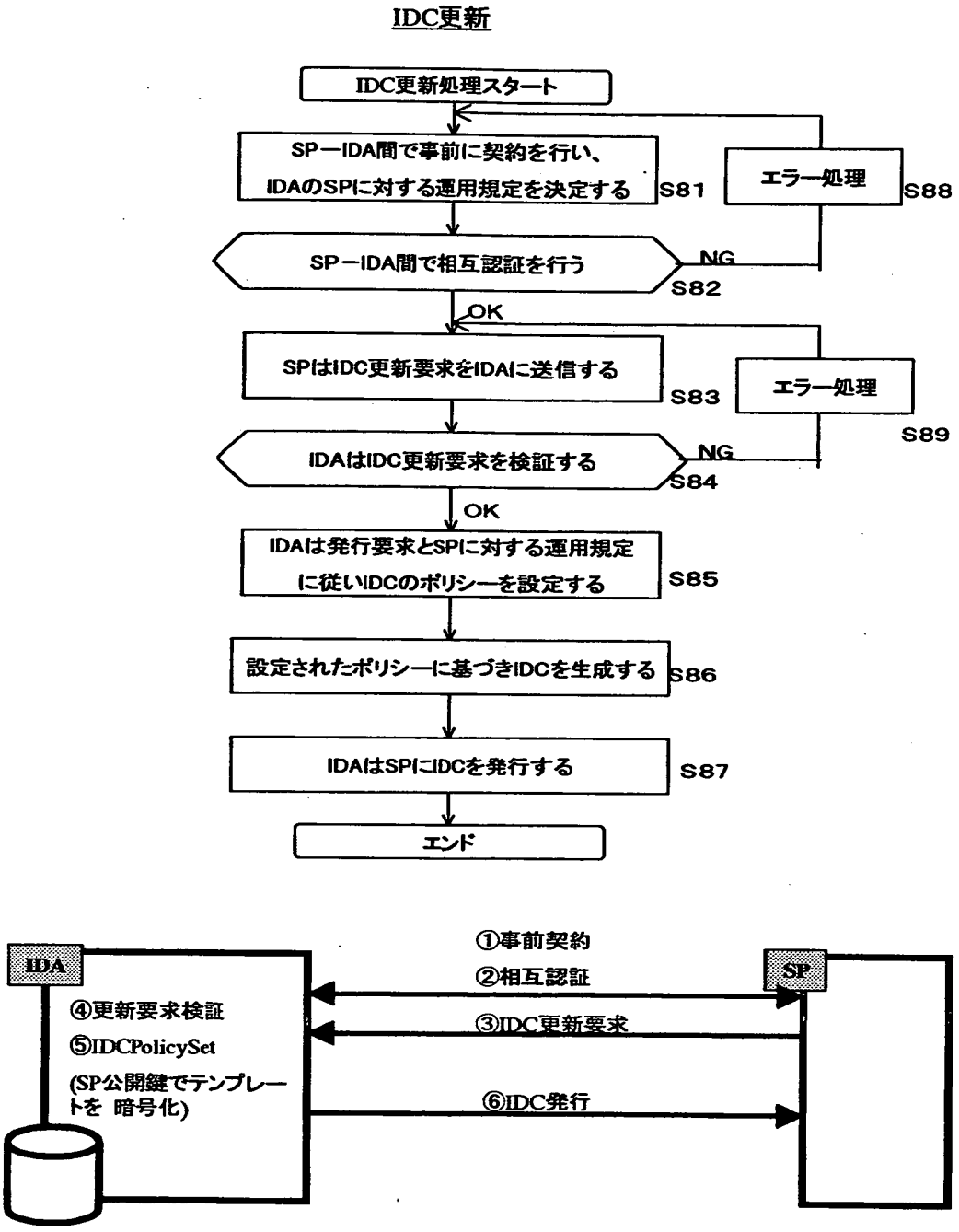
【図１４】


テンプレート停止解除
テンプレート停止解除処理スタート
ユーザはIDAにテンプレート再開要求を提出する
S61
ユーザは身元確認のための
個人証明データをIDAに提出する
S62
エラー処理
S67
ユーザは付加情報(PINなど)を
必要に応じてIDAに提出する
S63
IDAは提出されたデータの正当性を検証する
NG
S64
OK
IDAは登録されたテンプレート、個人証明データ、
付加情報の停止解除する
S65
IDAはユーザのIDCを失効を解除し
失効リストの更新を行う
S66
エンド
IDA
Template
受付
②提出データチェック
③個人データ停止解除
④失効リスト更新
個人証明
データ受付
①再開要求、個人証明データ、
付加情報提出

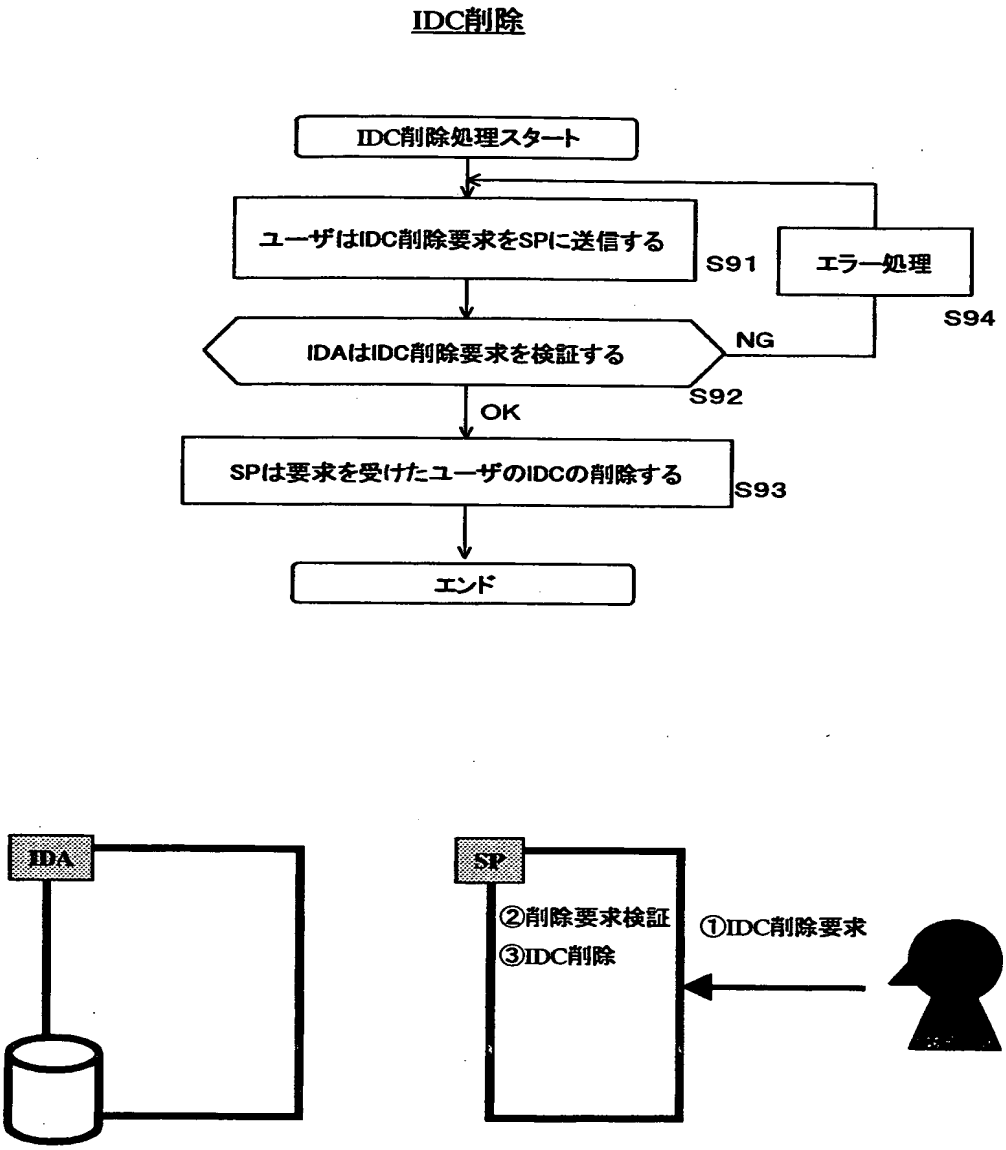
【図１５】


IDC配布
IDC配布1処理スタート
SP－IDA間で事前に契約を行い、
IDAのSPに対する運用規定を決定する
S71
エラー処理
S79
SP－IDA間で相互認証を行う
NG
S72
OK
SPはユーザ名とIDCのポリシーを
IDC発行要求としてIDAに送信する
S73
エラー処理
S80
IDAはIDC発行要求を検証する
NG
S74
OK
IDAは発行要求とSPに対する運用規定
に従いIDCのポリシーを設定する
S75
IDAの公開鍵で暗号化されている
テンプレートをSPの公開鍵で暗号化し直す
S76
設定されたポリシーに基づきIDCを生成する
S77
IDAはSPにIDCを発行する
S78
エンド
IDA
①事前契約
SP
②相互認証
③IDC発行要求
④発行要求検証
⑤IDCPolicySet
⑥SP公開鍵でテンプレートを 暗号化
⑦IDC発行
User

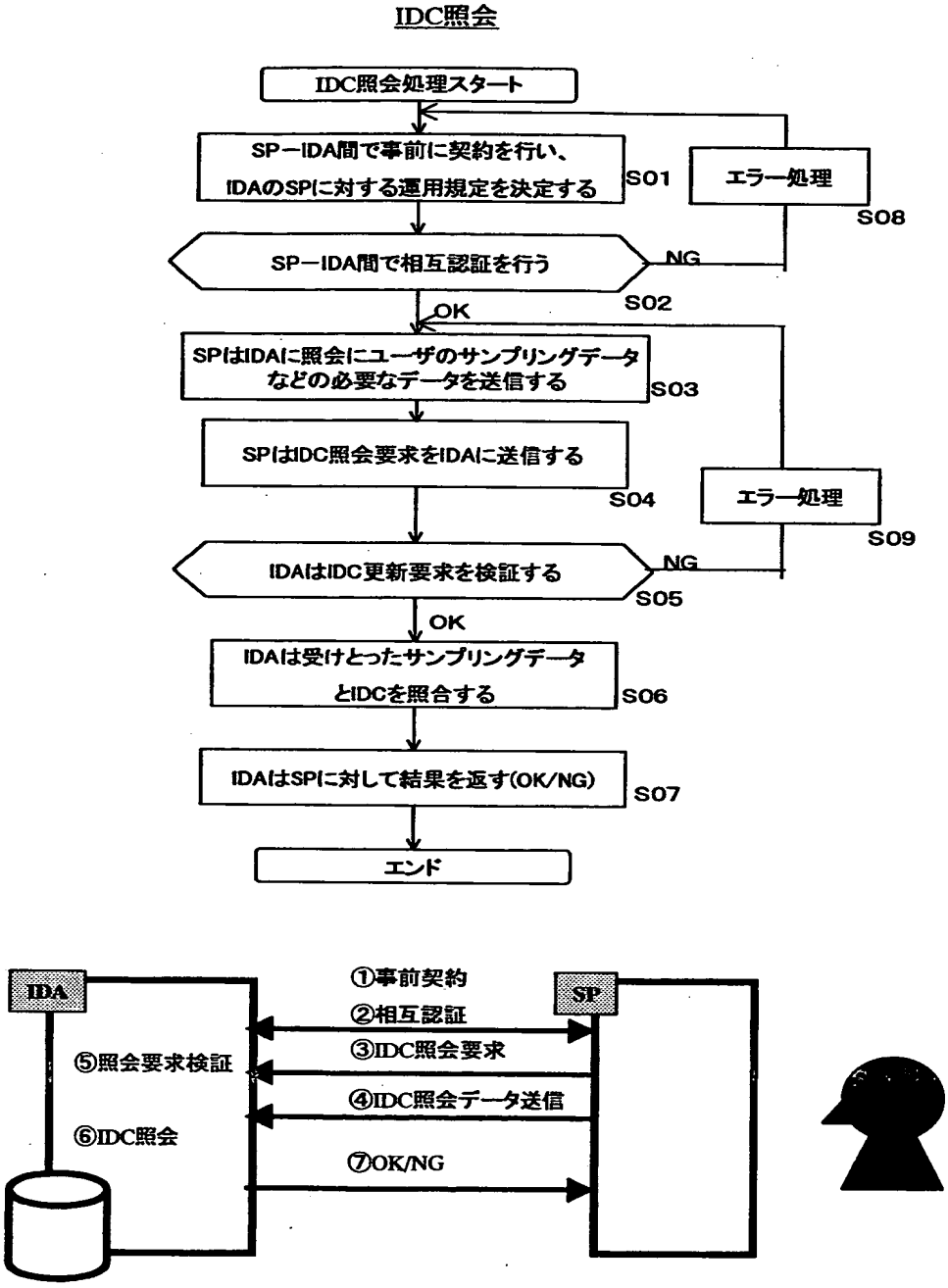
【図１６】


IDC更新
IDC更新処理スタート
SP－IDA間で事前に契約を行い、
IDAのSPに対する運用規定を決定する
S81
エラー処理
S88
SP－IDA間で相互認証を行う
NG
S82
OK
SPはIDC更新要求をIDAに送信する
S83
エラー処理
S89
IDAはIDC更新要求を検証する
NG
S84
OK
IDAは発行要求とSPに対する運用規定
に従いIDCのポリシーを設定する
S85
設定されたポリシーに基づきIDCを生成する
S86
IDAはSPにIDCを発行する
S87
エンド
IDA
④更新要求検証
⑤IDCPolicySet
(SP公開鍵でテンプレートを 暗号化)
①事前契約
②相互認証
③IDC更新要求
⑥IDC発行
SP

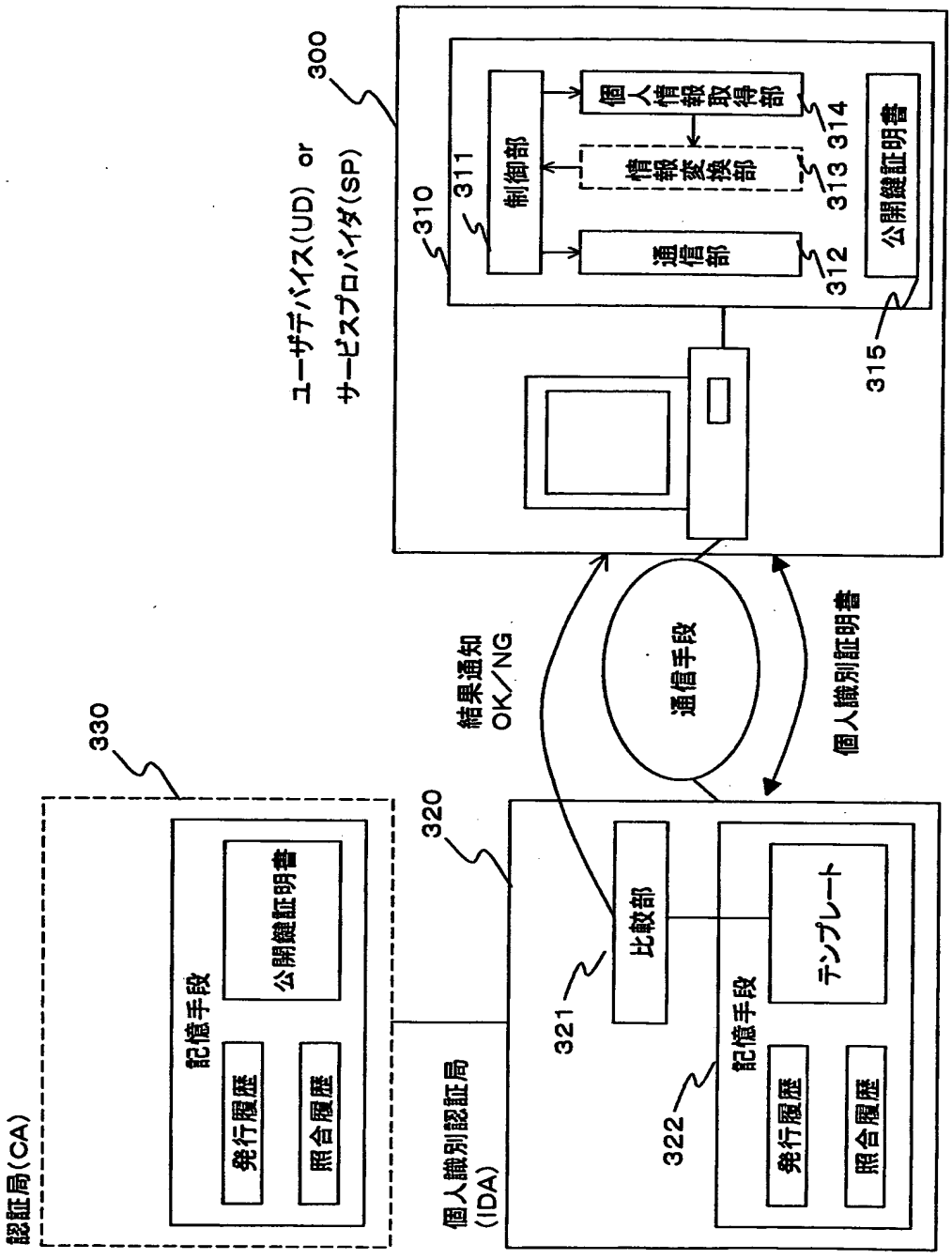
【図１７】


IDC削除
IDC削除処理スタート
ユーザはIDC削除要求をSPに送信する
S91
エラー処理
S94
IDAはIDC削除要求を検証する
NG
S92
OK
SPは要求を受けたユーザのIDCの削除する
S93
エンド
IDA
SP
②削除要求検証
③IDC削除
①IDC削除要求

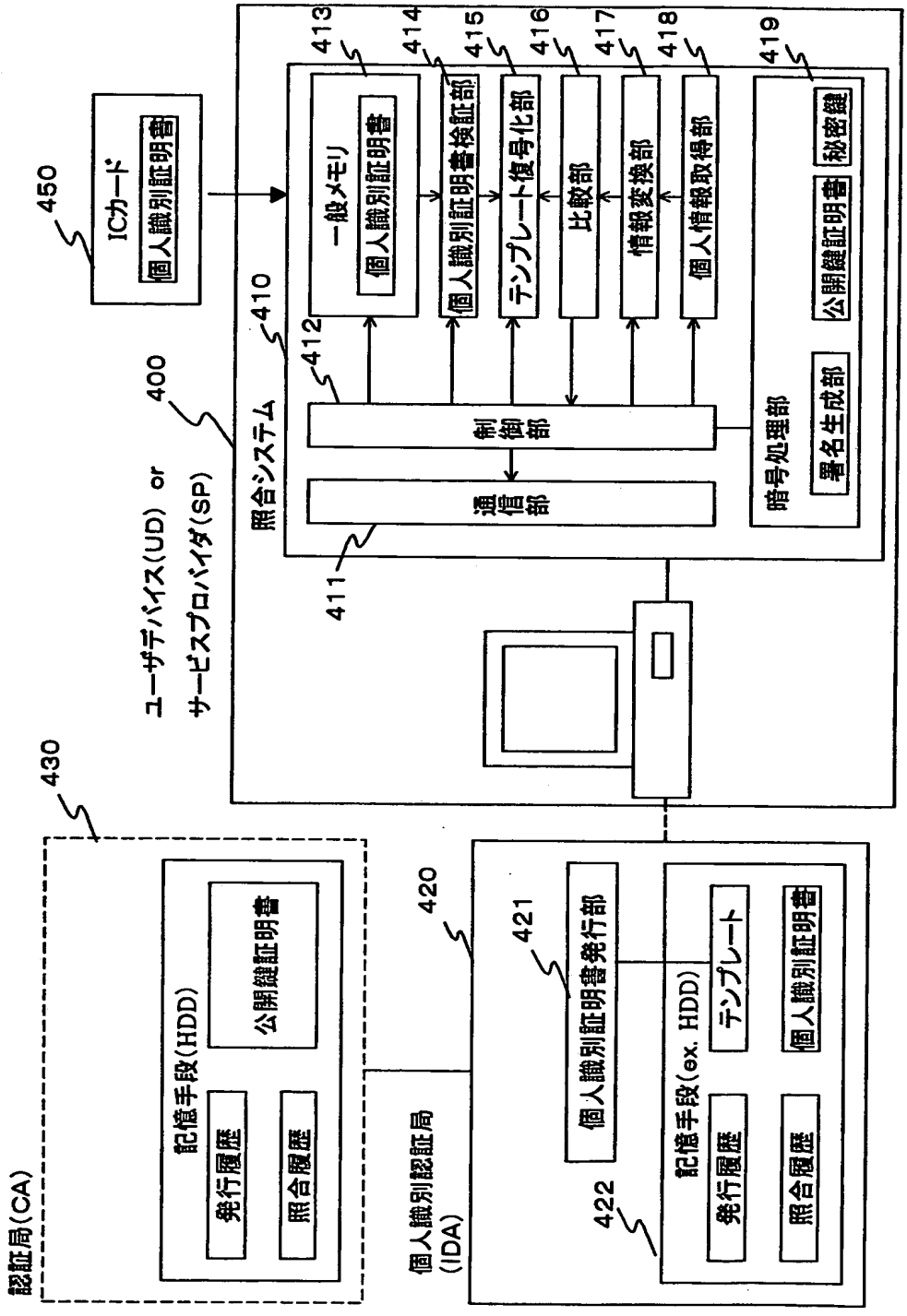
【図１８】


IDC照会
IDC照会処理スタート
SP－IDA間で事前に契約を行い、
IDAのSPに対する運用規定を決定する
S01
エラー処理
S08
SP－IDA間で相互認証を行う
NG
S02
OK
SPはIDAに照会にユーザのサンプリングデータ
などの必要なデータを送信する
S03
SPはIDC照会要求をIDAに送信する
S04
エラー処理
S09
IDAはIDC更新要求を検証する
NG
S05
OK
IDAは受けとったサンプリングデータ
とIDCを照合する
S06
IDAはSPに対して結果を返す(OK/NG)
S07
エンド
IDA
SP
①事前契約
②相互認証
③IDC照会要求
④IDC照会データ送信
⑤照会要求検証
⑥IDC照会
⑦OK/NG

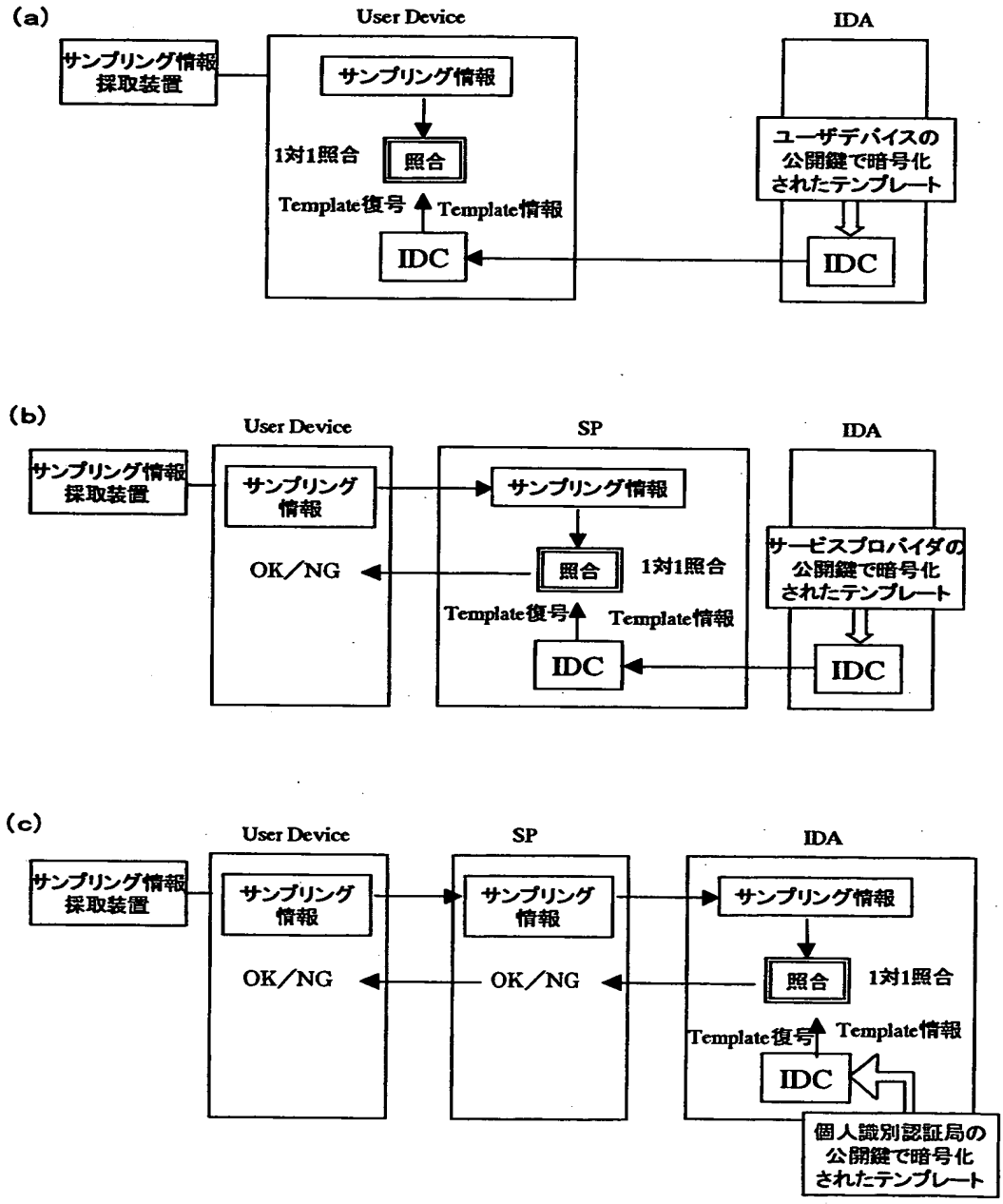
【図１９】


ユーザデバイス(UD) or
サービスプロバイダ(SP)
300
310
311
制御部
個人情報取得部
情報変換部
通信部
312
313
314
公開鍵証明書
315
通信手段
結果通知
OK／NG
個人識別証明書
320
比較部
321
テンプレート
記憶手段
322
発行履歴
照合履歴
個人識別認証局
(IDA)
330
記憶手段
公開鍵証明書
発行履歴
照合履歴
認証局(CA)

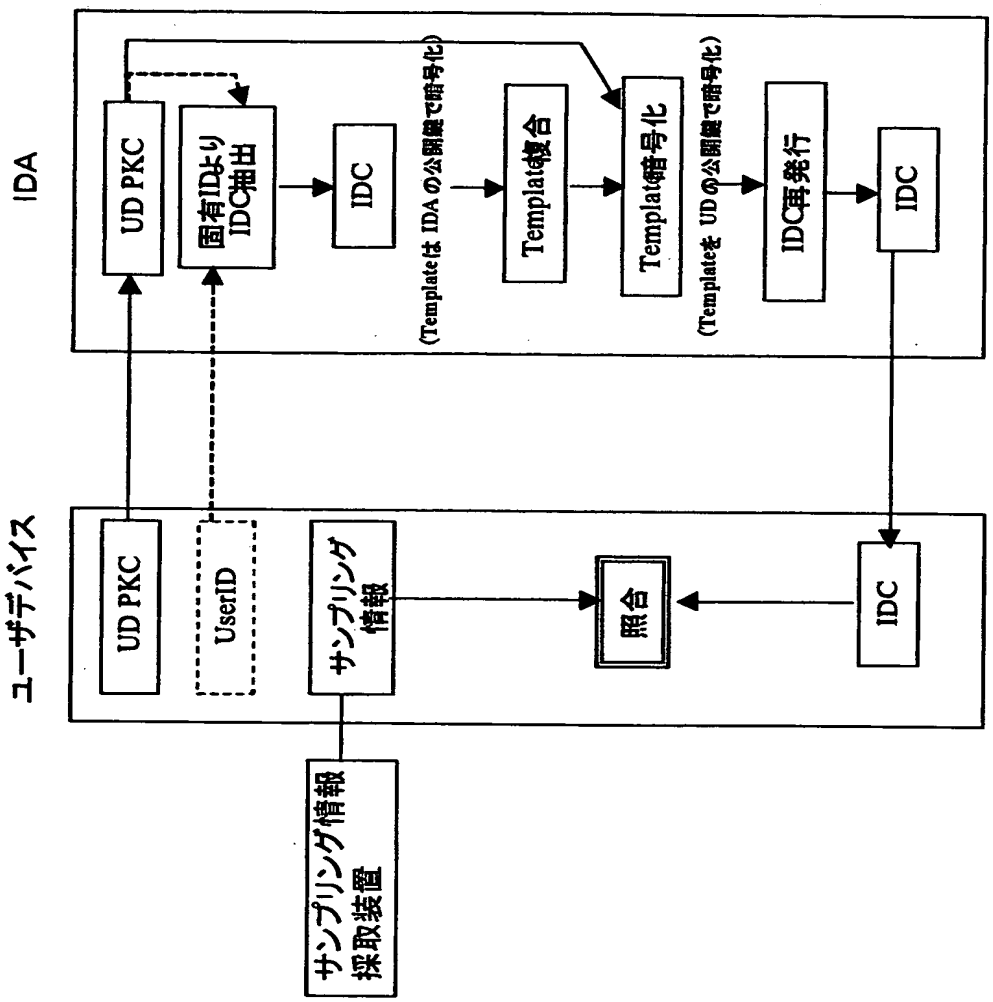
【図２０】


ICカード
個人識別証明書
450
ユーザデバイス(UD) or
サービスプロバイダ(SP)
400
照合システム
410
一般メモリ
個人識別証明書
413
412
414
個人識別証明書検証部
415
テンプレート復号化部
416
比較部
417
情報変換部
418
個人情報取得部
419
制御部
通信部
411
暗号処理部
署名生成部
公開鍵証明書
秘密鍵
430
認証局(CA)
記憶手段(HDD)
公開鍵証明書
発行履歴
照合履歴
420
個人識別認証局
(IDA)
421
個人識別証明書発行部
422
記憶手段(ex. HDD)
テンプレート
個人識別証明書
発行履歴
照合履歴

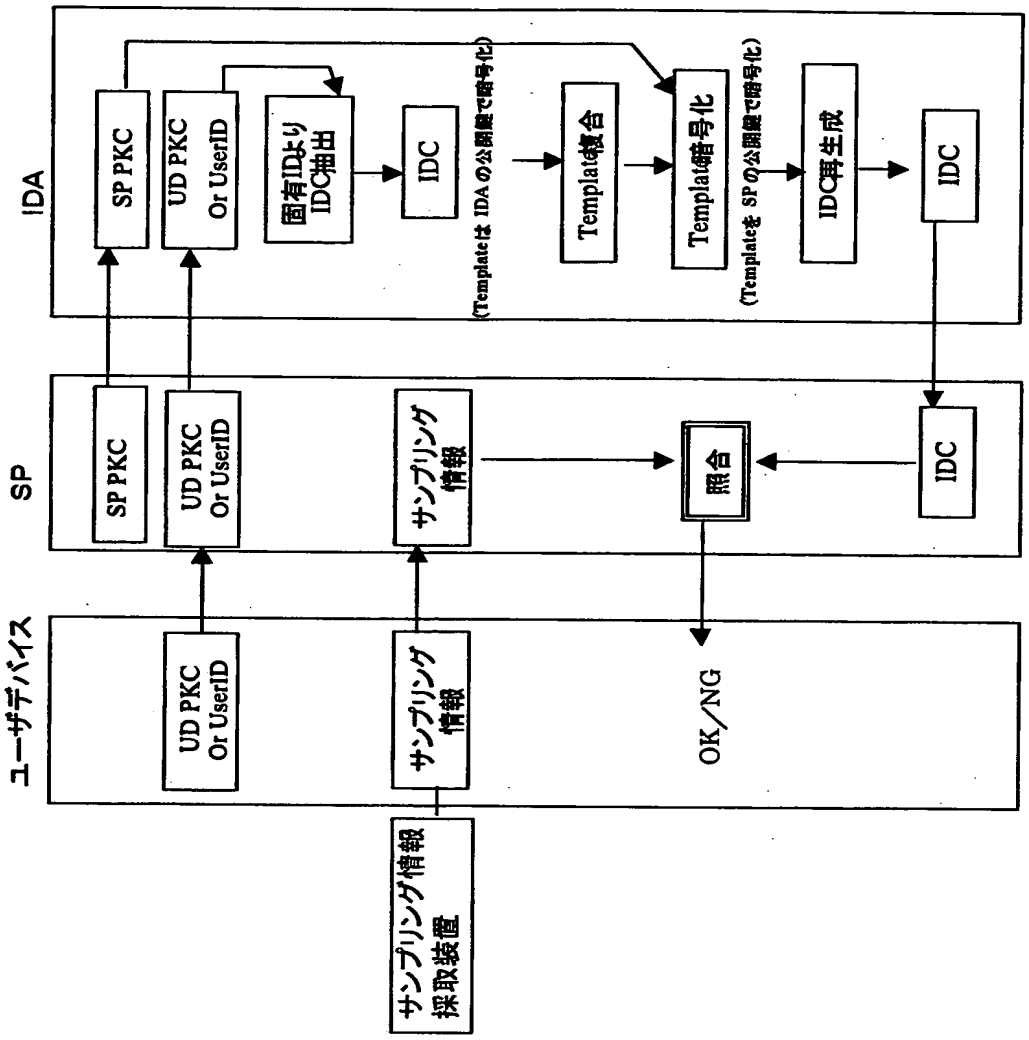
【図２１】


(a)
User Device
IDA
サンプリング情報採取装置
サンプリング情報
1対1照合
照合
Template復号
Template情報
IDC
ユーザデバイスの公開鍵で暗号化されたテンプレート
IDC
(b)
User Device
SP
IDA
サンプリング情報採取装置
サンプリング情報
サンプリング情報
OK／NG
照合
1対1照合
Template復号
Template情報
サービスプロバイダの公開鍵で暗号化されたテンプレート
IDC
IDC
(c)
User Device
SP
IDA
サンプリング情報採取装置
サンプリング情報
サンプリング情報
サンプリング情報
OK／NG
OK／NG
照合
1対1照合
Template復号
Template情報
IDC
個人識別認証局の公開鍵で暗号化されたテンプレート

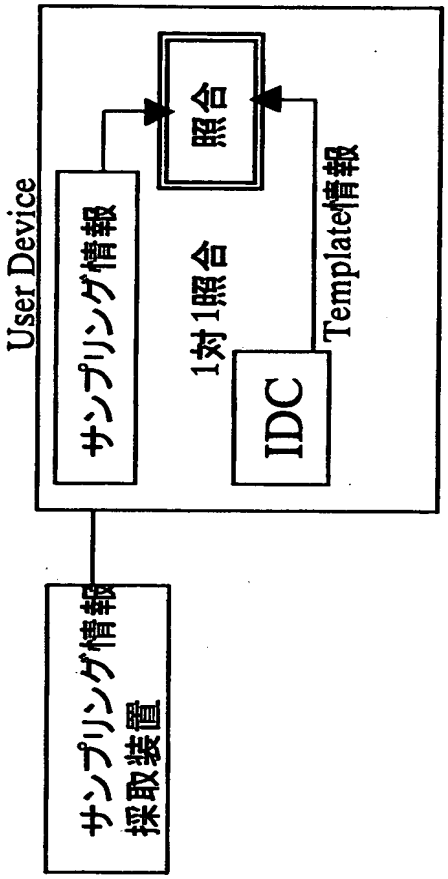
【図２２】


IDA
UD PKC
固有IDより
IDC抽出
IDC
(TemplateはIDAの公開鍵で暗号化)
Template複合
Template暗号化
(TemplateをUDの公開鍵で暗号化)
IDC再発行
IDC
ユーザデバイス
UD PKC
UserID
サンプリング
情報
照合
IDC
サンプリング情報
採取装置

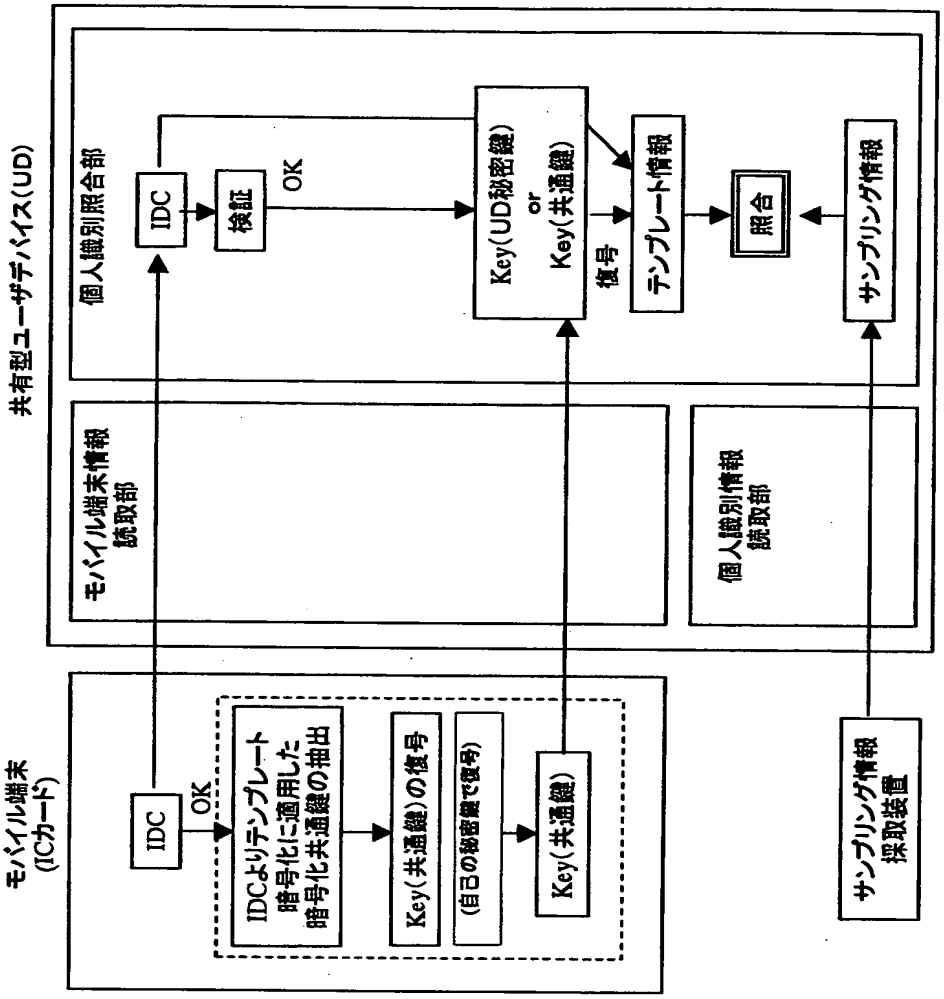
【図２３】


IDA
SP PKC
UD PKC Or UserID
固有IDより IDC抽出
IDC
(Templateは IDA の公開鍵で暗号化)
Templat複合
Templat暗号化
(Templateを SP の公開鍵で暗号化)
IDC再生成
IDC
SP
SP PKC
UD PKC Or UserID
サンプリング情報
照合
IDC
ユーザデバイス
UD PKC Or UserID
サンプリング情報
OK／NG
サンプリング情報採取装置

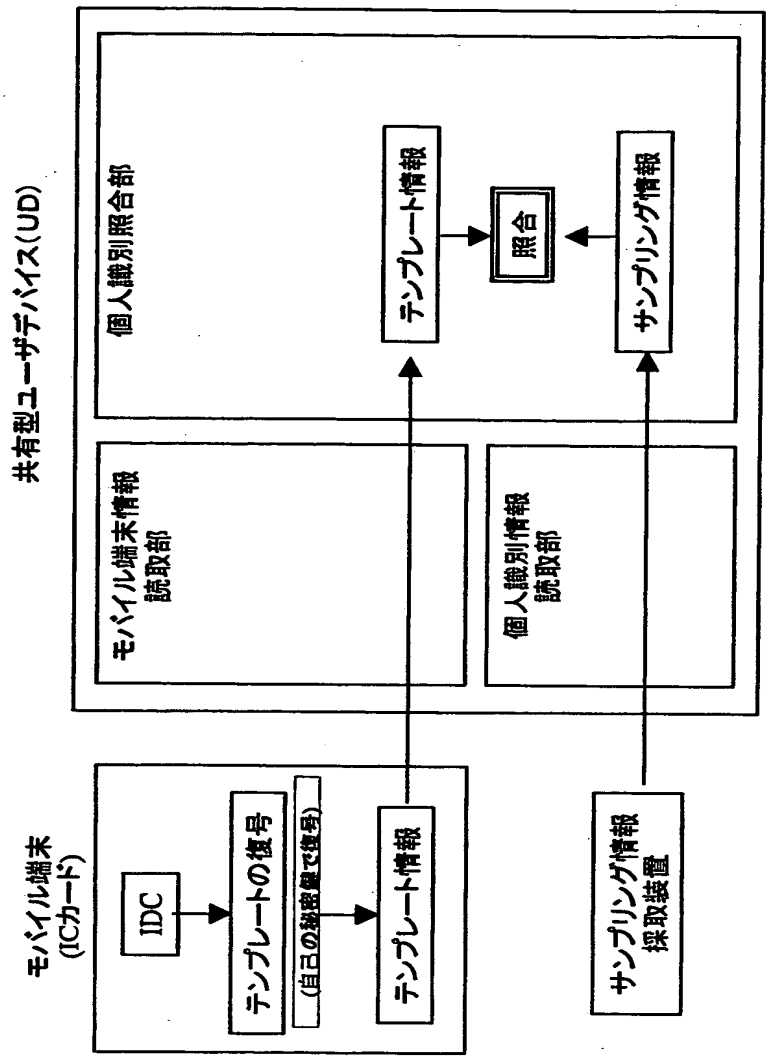
【図２４】


User Device
照合
サンプリング情報
1対1照合
Template情報
IDC
サンプリング情報
採取装置

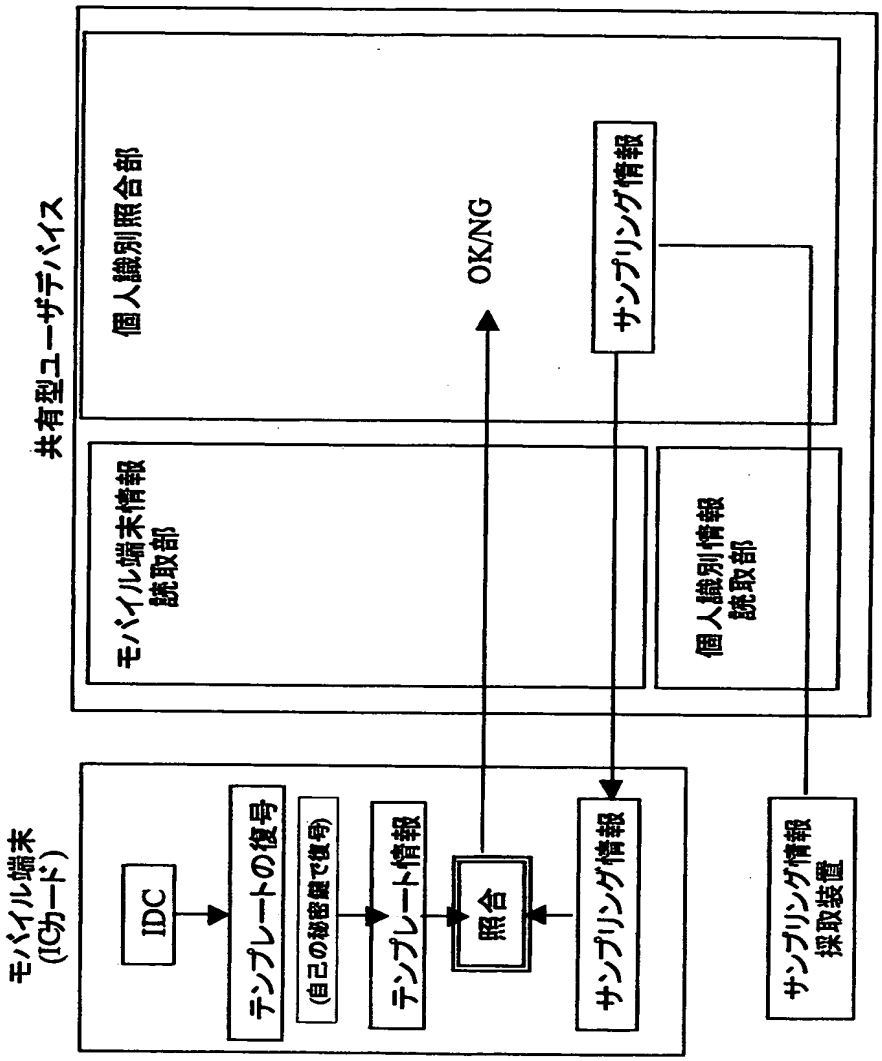
【図２５】


共有型ユーザデバイス(UD)
個人識別照合部
IDC
検証
OK
Key(UD秘密鍵)
or
Key(共通鍵)
復号
テンプレート情報
照合
サンプリング情報
モバイル端末情報
読取部
個人識別情報
読取部
モバイル端末
(ICカード)
IDC
OK
IDCよりテンプレート
暗号化に適用した
暗号化共通鍵の抽出
Key(共通鍵)の復号
(自己の秘密鍵で復号)
Key(共通鍵)
サンプリング情報
採取装置

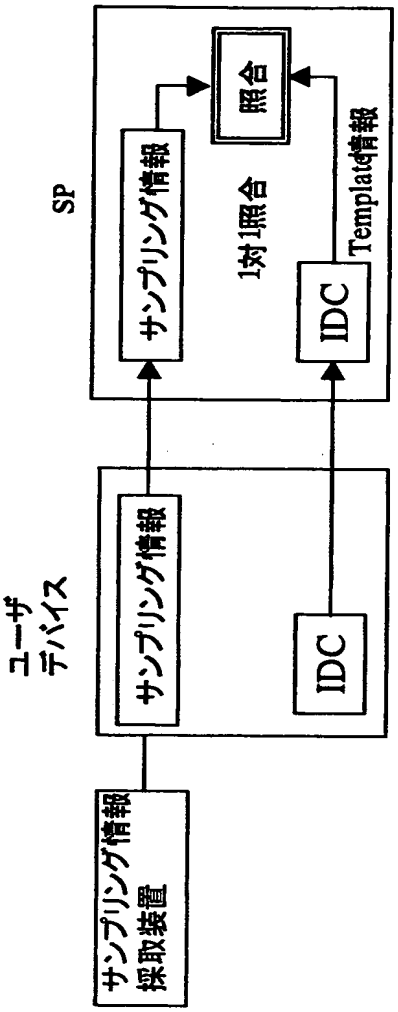
【図２６】


共有型ユーザデバイス(UD)
個人識別照合部
テンプレート情報
照合
サンプリング情報
モバイル端末情報
読取部
個人識別情報
読取部
モバイル端末
(ICカード)
IDC
テンプレートの復号
(自己の秘密鍵で復号)
テンプレート情報
サンプリング情報
採取装置

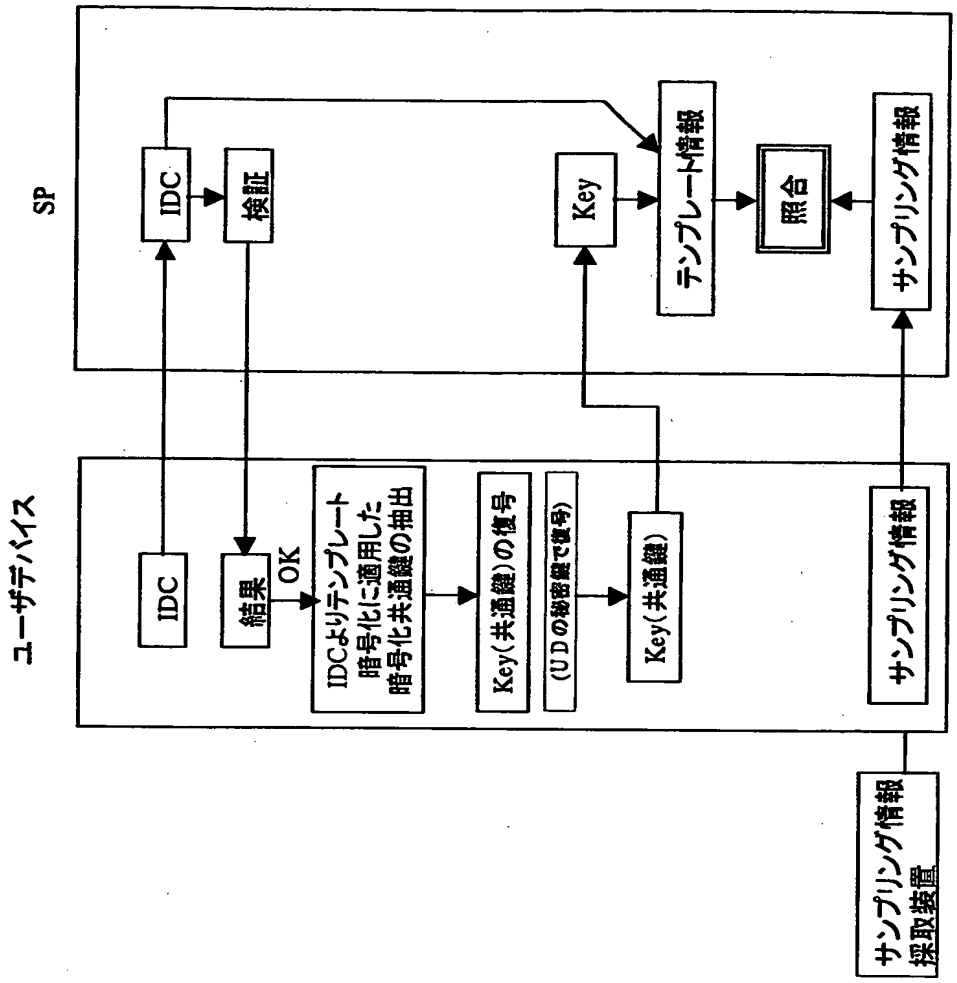
【図２７】


共有型ユーザデバイス
個人識別照合部
モバイル端末情報
読取部
個人識別情報
読取部
OK/NG
サンプリング情報
モバイル端末
(ICカード)
IDC
テンプレートの復号
(自己の秘密鍵で復号)
テンプレート情報
照合
サンプリング情報
サンプリング情報
採取装置

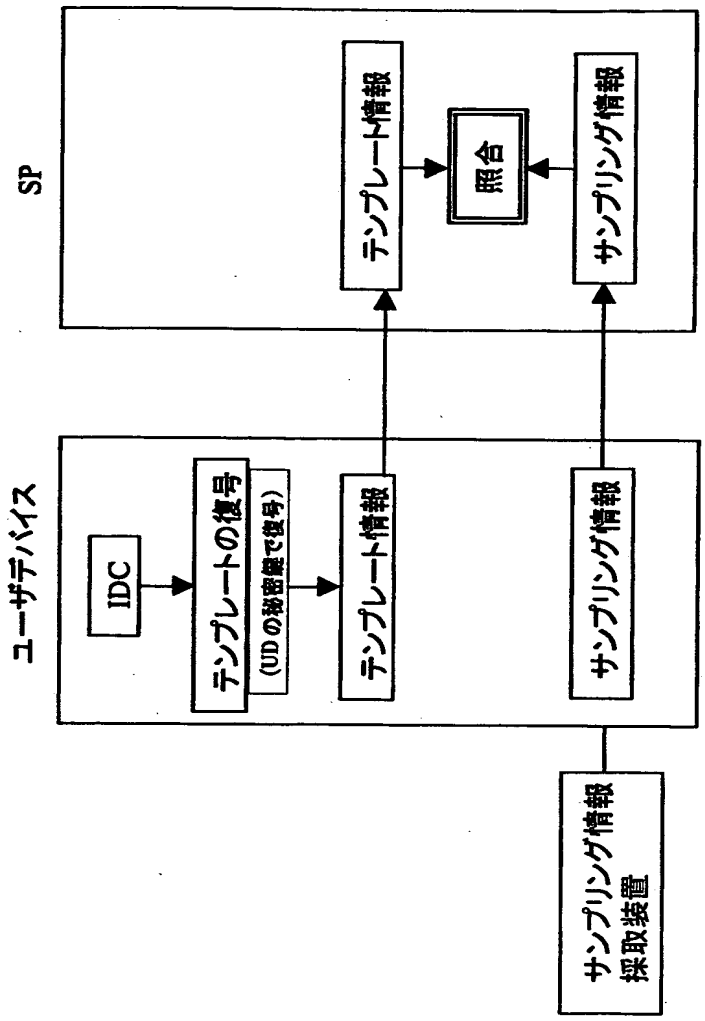
【図２８】


SP
照合
サンプリング情報
1対1照合
IDC
Template情報
ユーザ
デバイス
サンプリング情報
IDC
サンプリング情報
採取装置

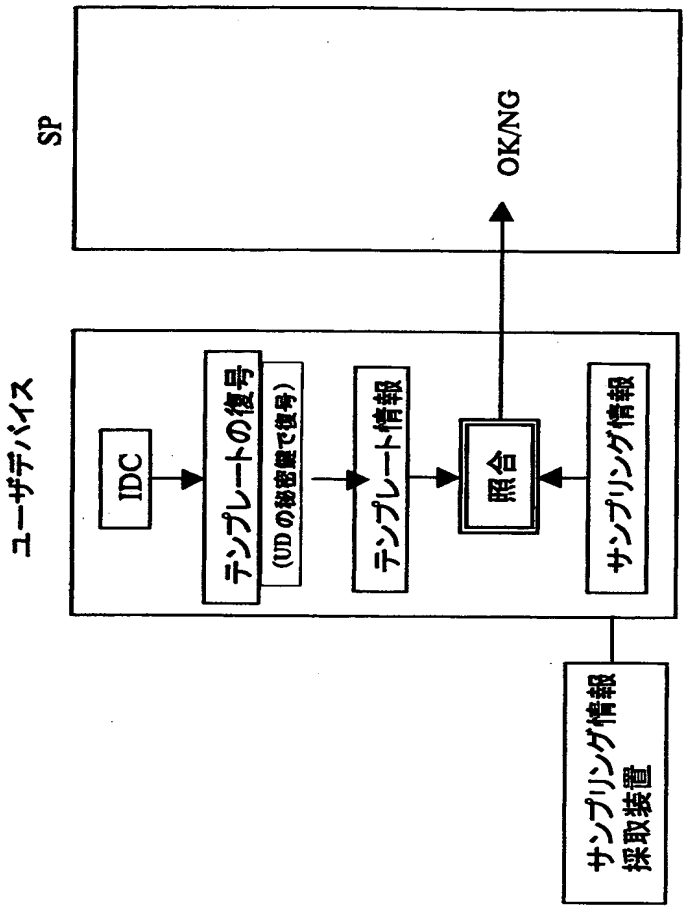
【図２９】


SP
IDC
検証
Key
テンプレート情報
照合
サンプリング情報
ユーザデバイス
IDC
結果
OK
IDCよりテンプレート
暗号化に適用した
暗号化共通鍵の抽出
Key(共通鍵)の復号
(UDの秘密鍵で復号)
Key(共通鍵)
サンプリング情報
サンプリング情報
採取装置

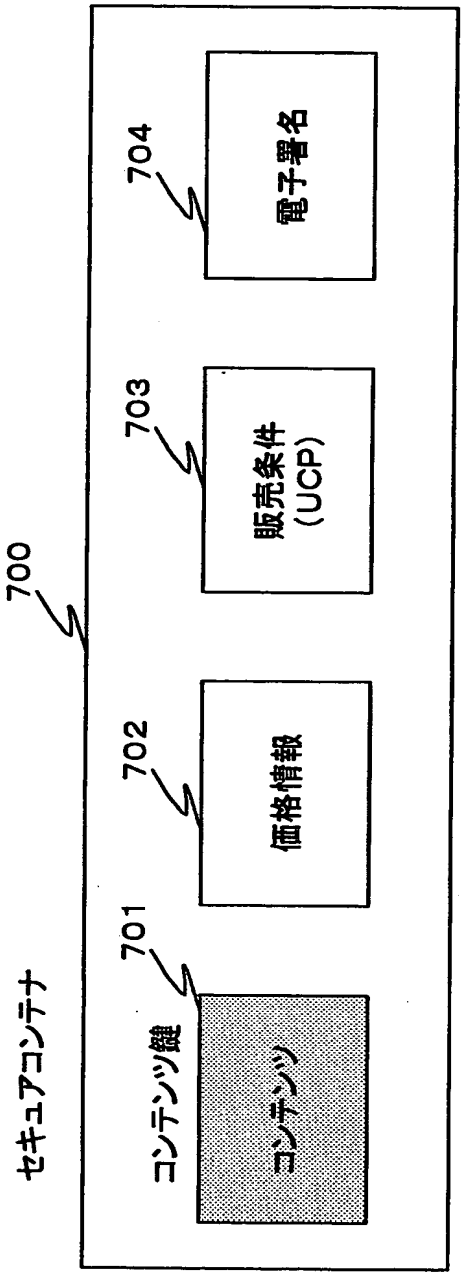
【図３０】


SP
テンプレート情報
照合
サンプリング情報
ユーザデバイス
IDC
テンプレートの復号
(UDの秘密鍵で復号)
テンプレート情報
サンプリング情報
サンプリング情報
採取装置

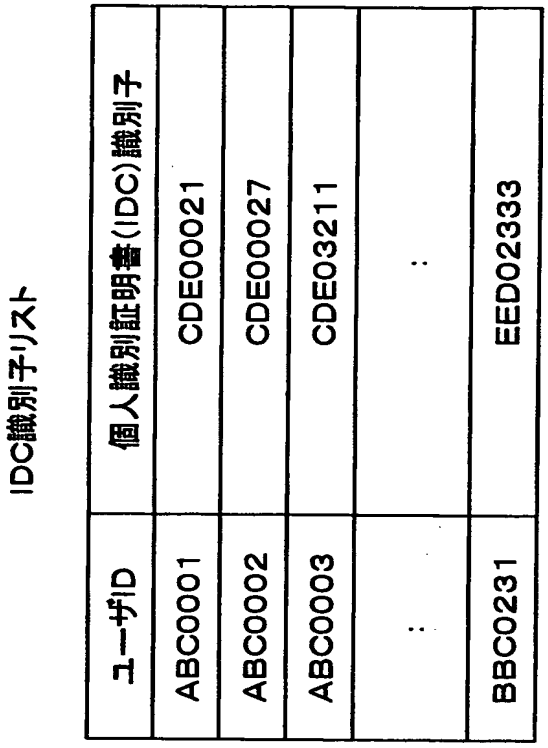
【図３１】


SP
OK/NG
ユーザデバイス
IDC
テンプレートの復号
(IDの秘密鍵で復号)
テンプレート情報
照合
サンプリング情報
サンプリング情報
採取装置

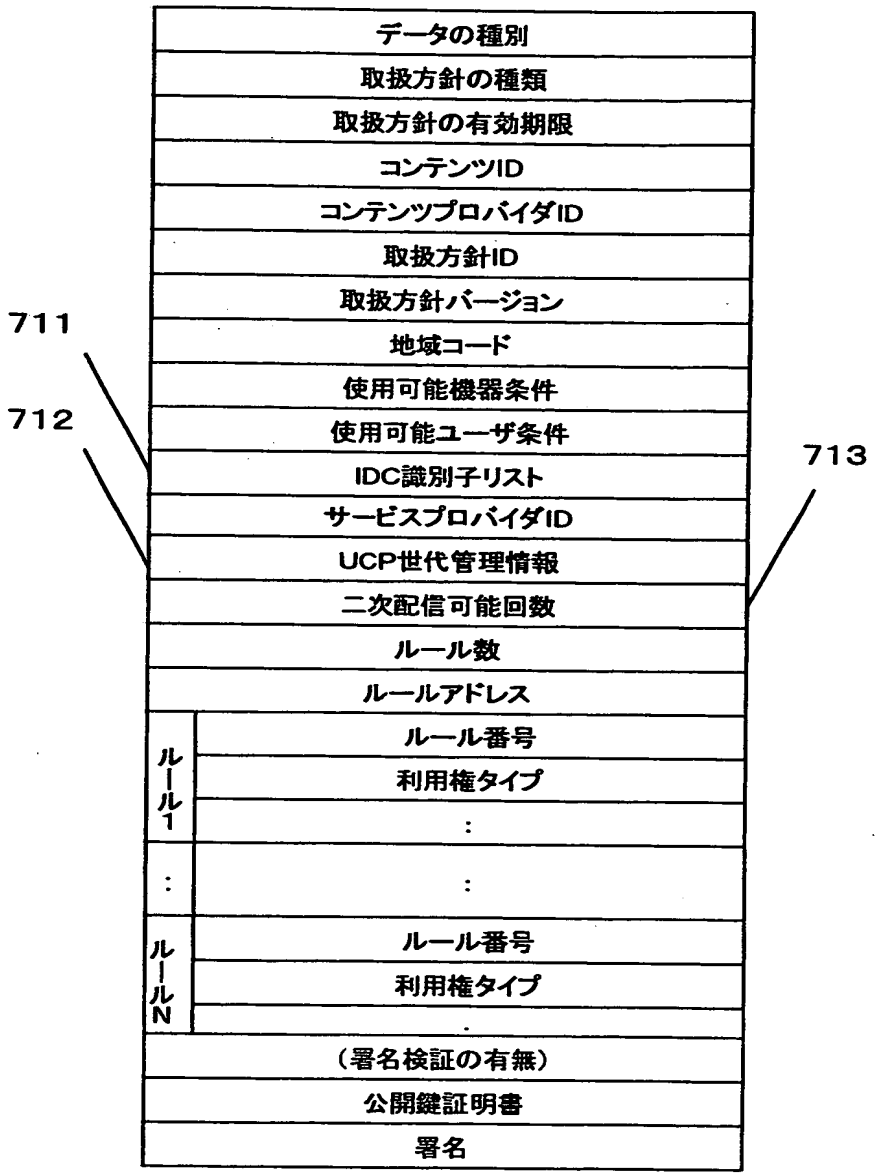
【図３２】



【図３３】


IDC識別子リスト
ユーザID
個人識別証明書(IDC)識別子
ABC0001
CDE00021
ABC0002
CDE00027
ABC0003
CDE03211
BBC0231
EED02333

【図３４】

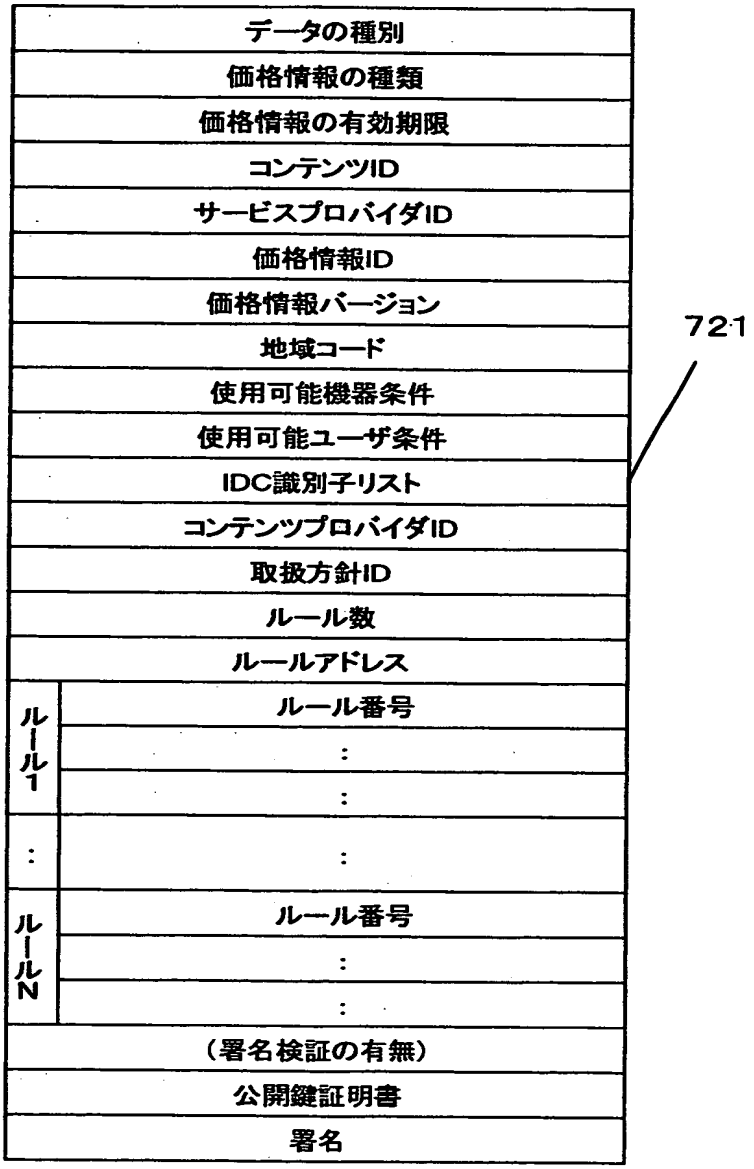


UCP(販売条件情報)

【図３５】

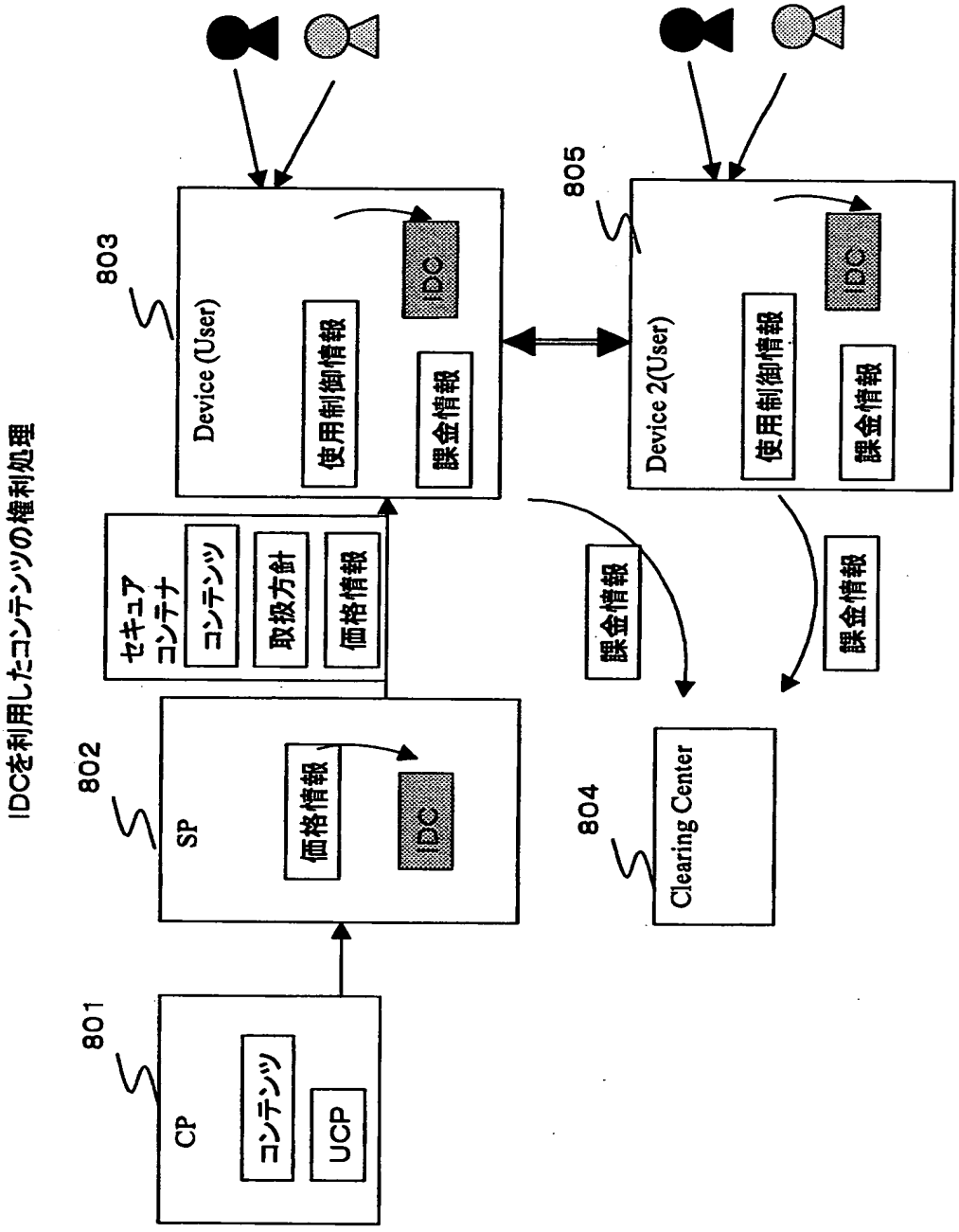
ルール番号	利用権の内容	期間制限	回数制限	複製制限
1	再生権	なし	なし	－
2		あり	なし	－
3		なし	あり	－
4	複製権	なし	なし	なし
5		あり	なし	なし
6		なし	あり	なし
7		なし	なし	SCMS
8		あり	なし	
9		なし	あり	
10		なし	なし	その他
11		あり	なし	
12		なし	あり	
13	権利内容変更			
14	再配布			
15	アルバム化アップグレード			
16	管理移動権			

【図３６】

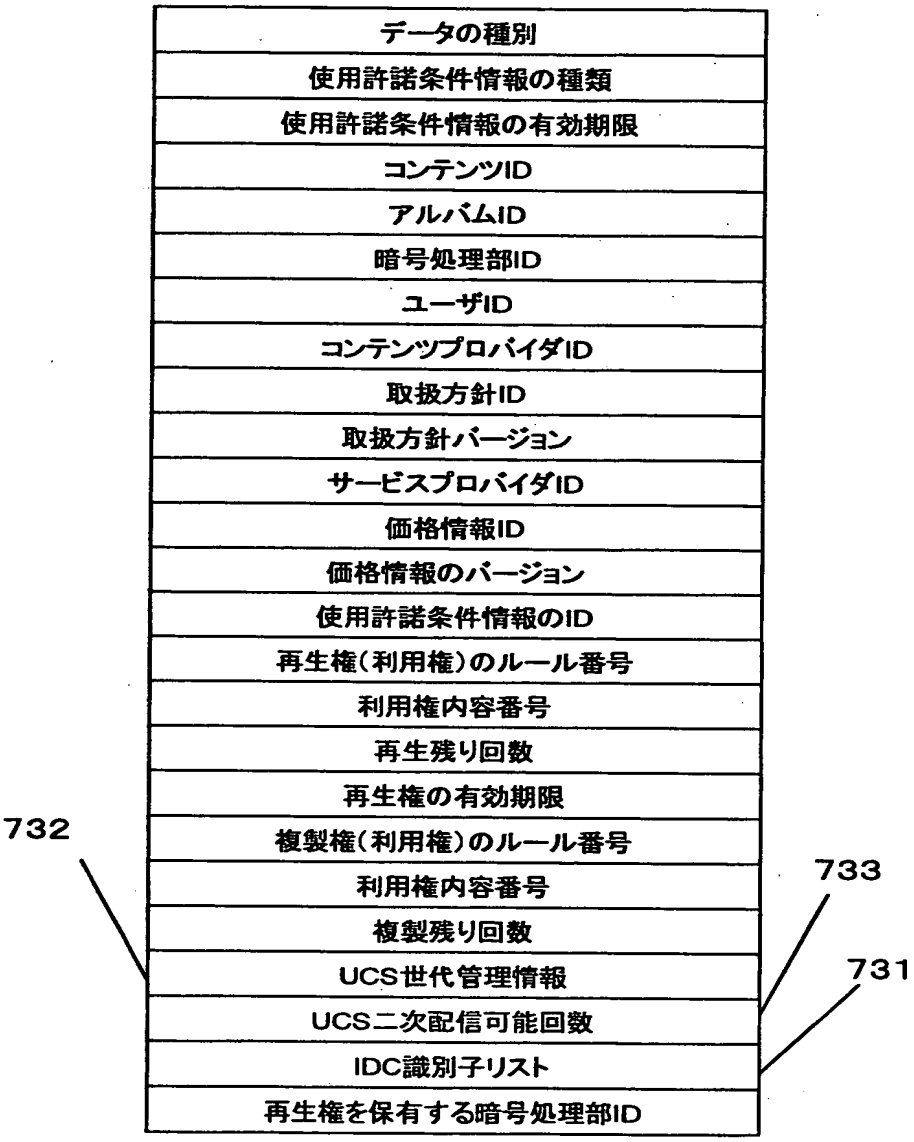

データの種別
価格情報の種類
価格情報の有効期限
コンテンツID
サービスプロバイダID
価格情報ID
価格情報バージョン
地域コード
使用可能機器条件
使用可能ユーザ条件
IDC識別子リスト
コンテンツプロバイダID
取扱方針ID
ルール数
ルールアドレス
ルール1
ルール番号
:
:
:
:
ルールN
ルール番号
:
:
（署名検証の有無）
公開鍵証明書
署名
721

価格情報

【図３７】

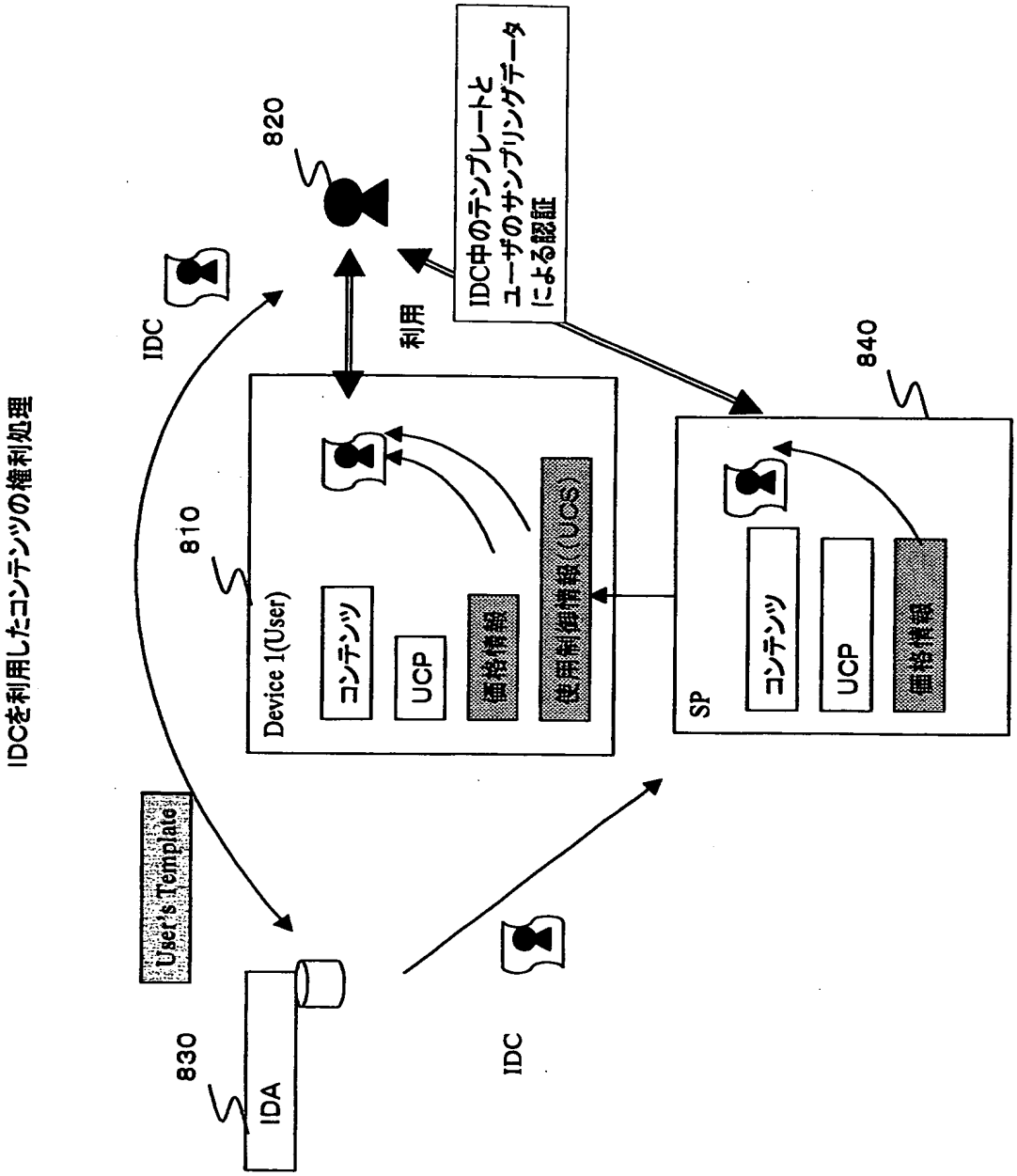

IDCを利用したコンテンツの権利処理
801
CP
コンテンツ
UCP
802
SP
価格情報
IDC
803
Device (User)
使用制御情報
IDC
課金情報
805
Device 2(User)
使用制御情報
IDC
課金情報
セキュア
コンテナ
コンテンツ
取扱方針
価格情報
課金情報
課金情報
804
Clearing Center

【図３８】

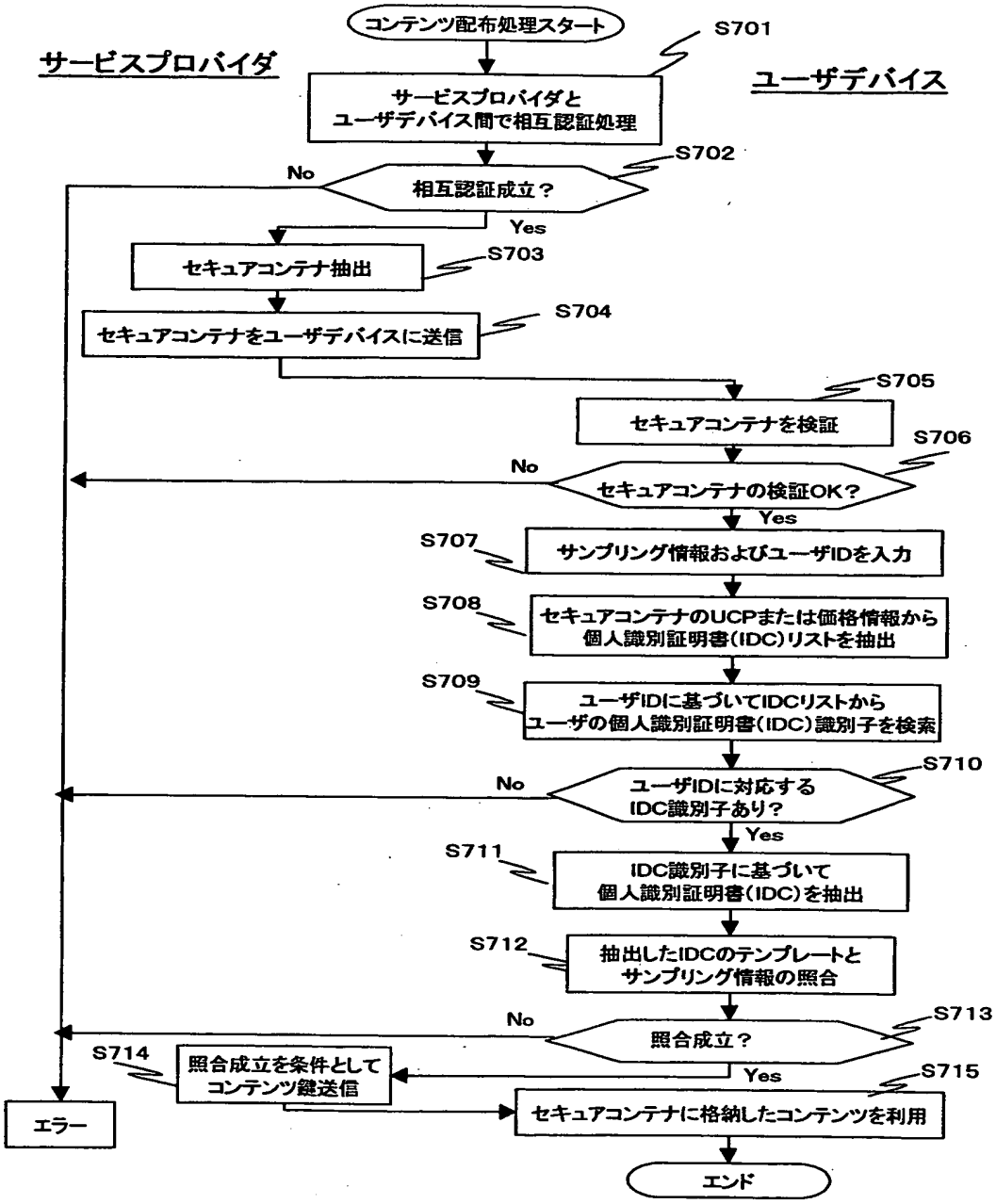


UCS（使用制御情報）

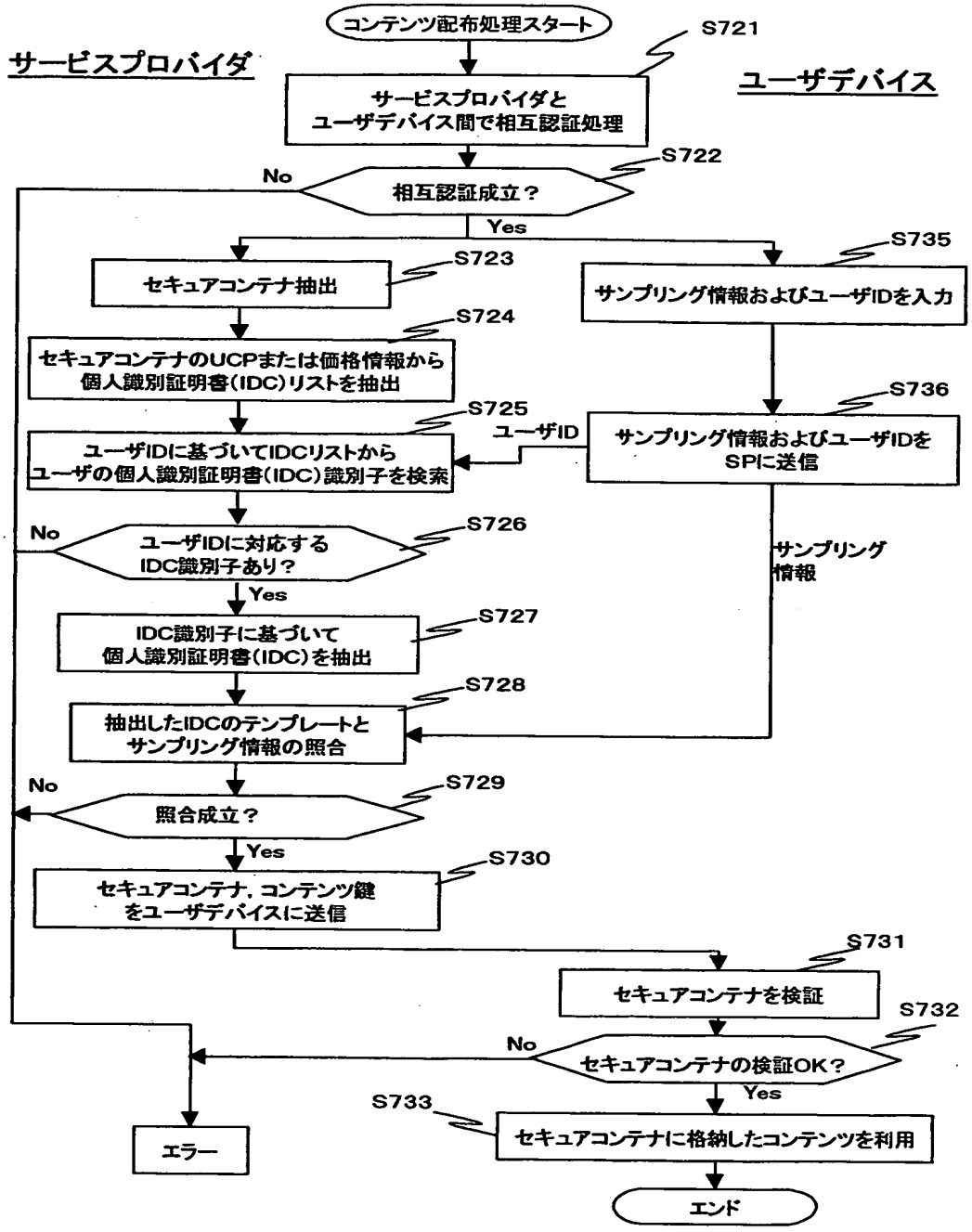
【図３９】


IDCを利用したコンテンツの権利処理
IDC
820
IDC中のテンプレートと
ユーザのサンプリングデータ
による認証
利用
840
810
Device 1(User)
コンテンツ
UCP
固有情報
使用制御情報(UCS)
SP
コンテンツ
UCP
固有情報
User's Template
830
IDA
IDC

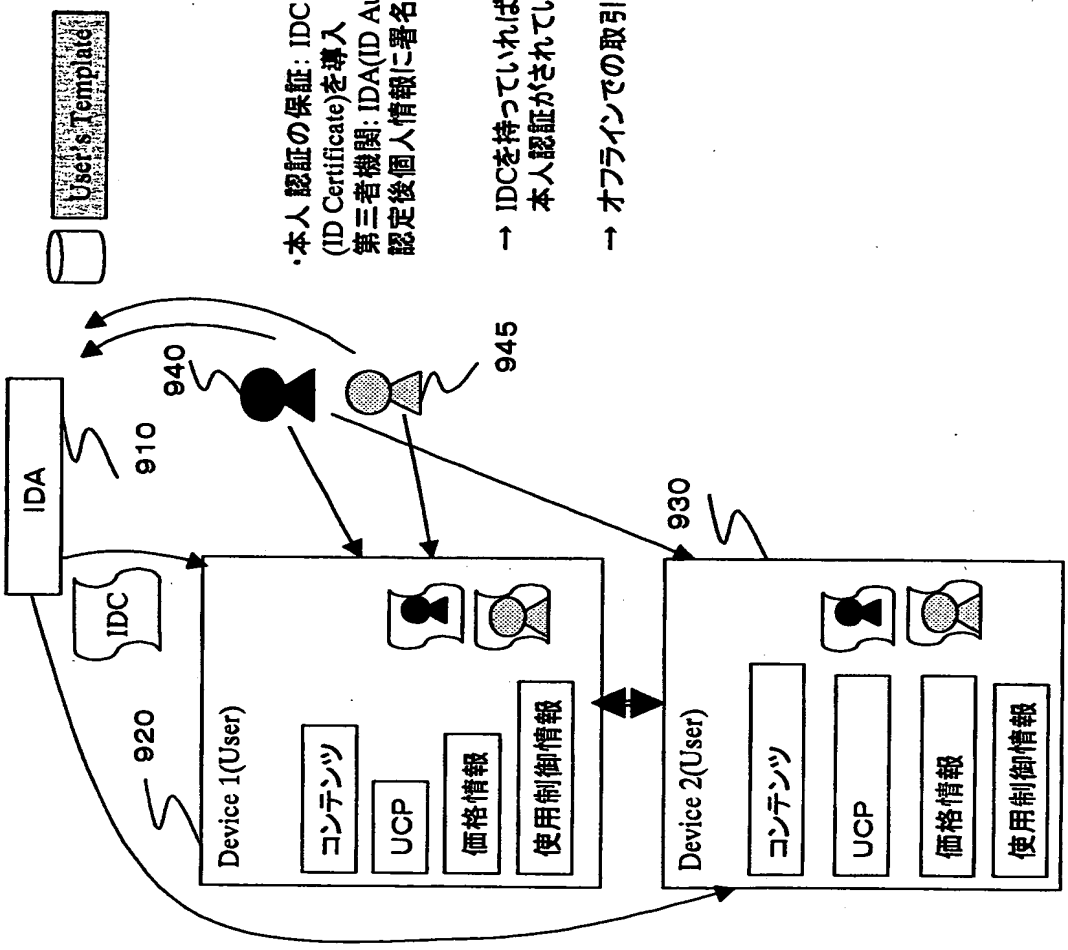
【図４０】


コンテンツ配布処理スタート
S701
サービスプロバイダ
ユーザデバイス
サービスプロバイダと
ユーザデバイス間で相互認証処理
S702
No
相互認証成立？
Yes
セキュアコンテナ抽出
S703
セキュアコンテナをユーザデバイスに送信
S704
S705
セキュアコンテナを検証
S706
No
セキュアコンテナの検証OK？
Yes
S707
サンプリング情報およびユーザIDを入力
S708
セキュアコンテナのUCPまたは価格情報から
個人識別証明書(IDC)リストを抽出
S709
ユーザIDに基づいてIDCリストから
ユーザの個人識別証明書(IDC)識別子を検索
S710
No
ユーザIDに対応する
IDC識別子あり？
Yes
S711
IDC識別子に基づいて
個人識別証明書(IDC)を抽出
S712
抽出したIDCのテンプレートと
サンプリング情報の照合
No
S713
照合成立？
S714
照合成立を条件として
コンテンツ鍵送信
Yes
S715
エラー
セキュアコンテナに格納したコンテンツを利用
エンド

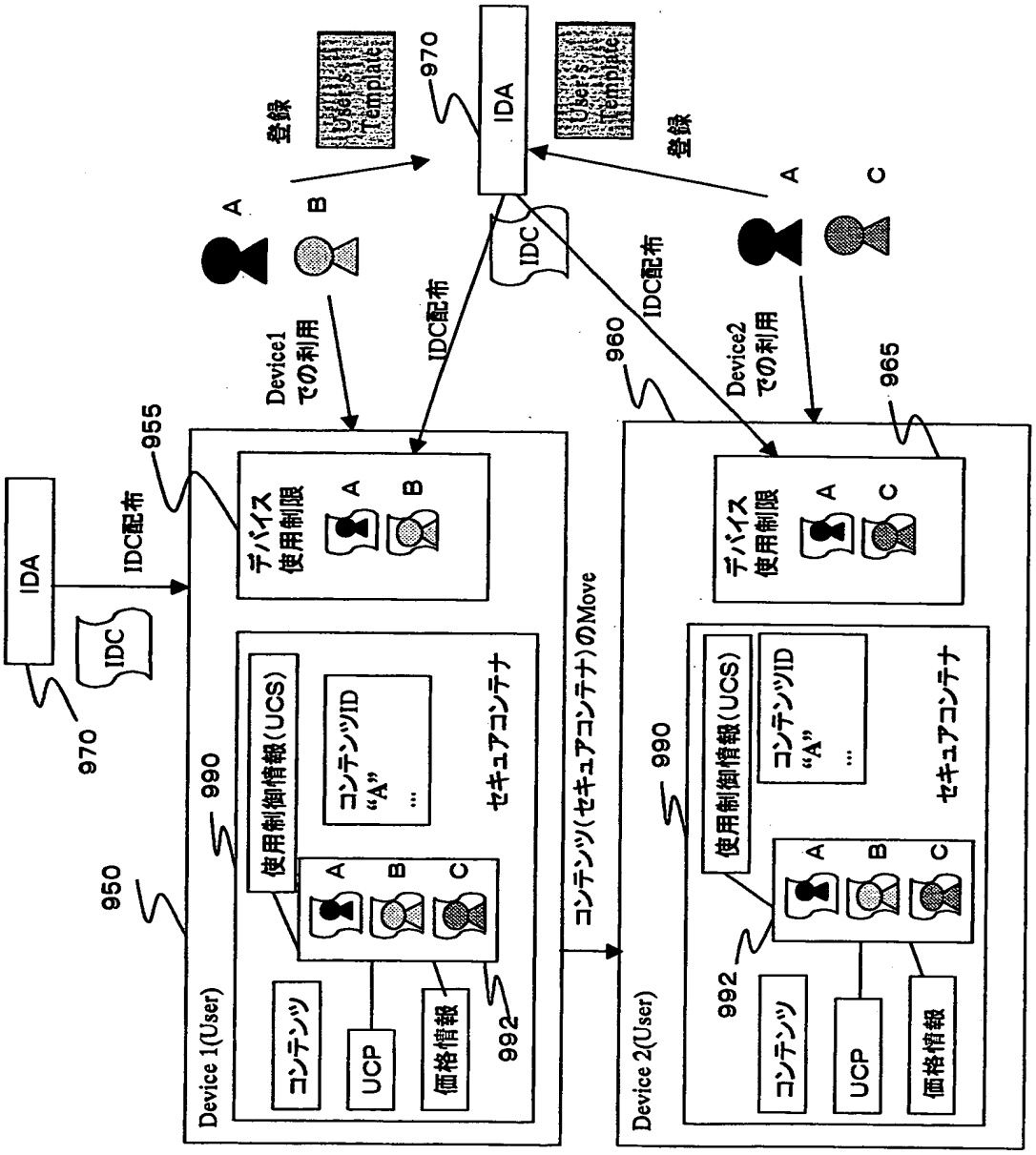
【図４１】


コンテンツ配布処理スタート
サービスプロバイダ
ユーザデバイス
S721
サービスプロバイダと
ユーザデバイス間で相互認証処理
S722
No
相互認証成立？
Yes
S723
セキュアコンテナ抽出
S735
サンプリング情報およびユーザIDを入力
S724
セキュアコンテナのUCPまたは価格情報から
個人識別証明書(IDC)リストを抽出
S736
S725
ユーザID
ユーザIDに基づいてIDCリストから
ユーザの個人識別証明書(IDC)識別子を検索
サンプリング情報およびユーザIDを
SPに送信
No
S726
ユーザIDに対応する
IDC識別子あり？
サンプリング
情報
Yes
S727
IDC識別子に基づいて
個人識別証明書(IDC)を抽出
S728
抽出したIDCのテンプレートと
サンプリング情報の照合
No
S729
照合成立？
Yes
S730
セキュアコンテナ，コンテンツ鍵
をユーザデバイスに送信
S731
セキュアコンテナを検証
S732
No
セキュアコンテナの検証OK？
Yes
S733
エラー
セキュアコンテナに格納したコンテンツを利用
エンド

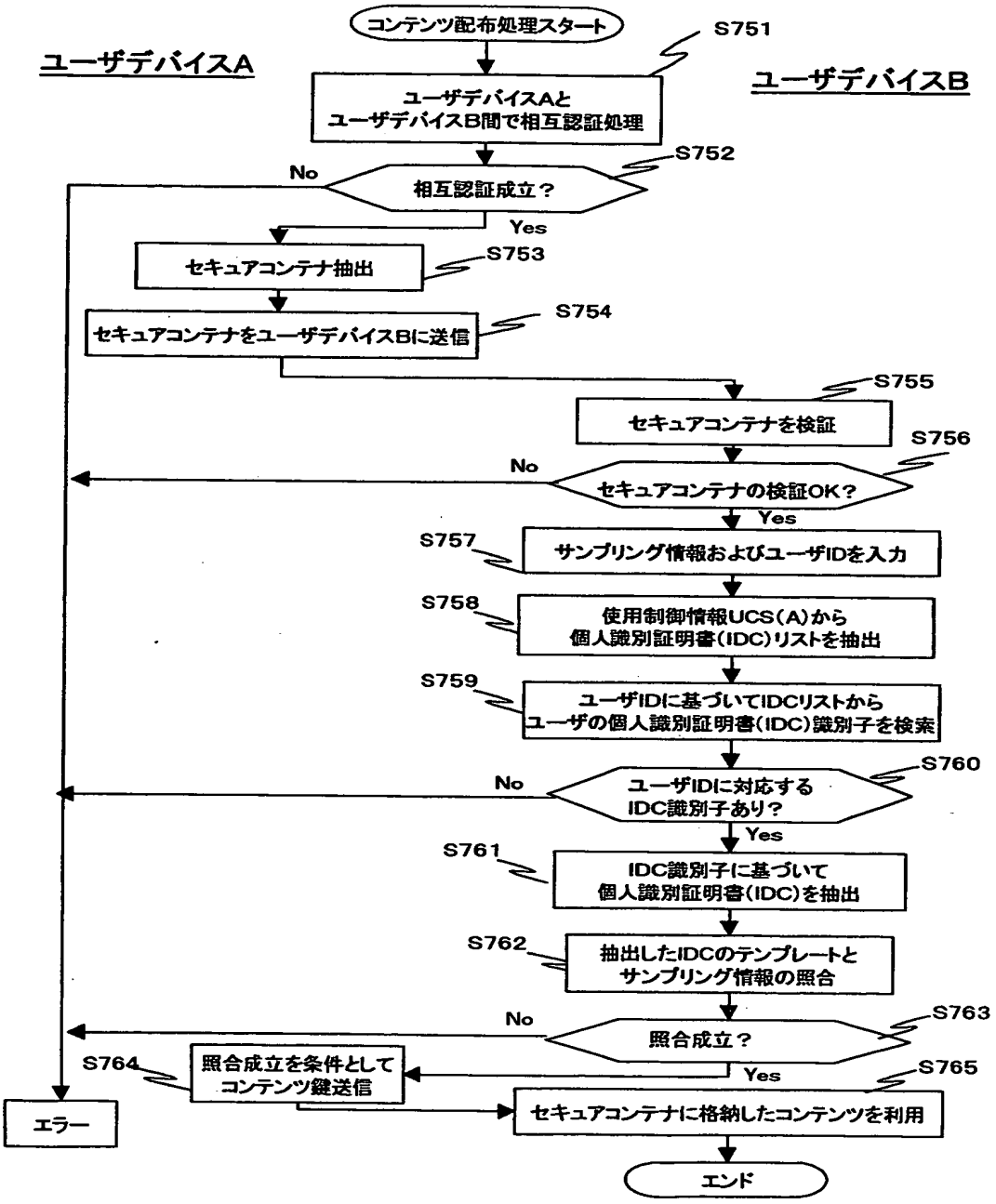
【図４２】


User's Template
・本人認証の保証：IDC
(ID Certificate)を導入
第三者機関：IDA(ID Authority)が本人を
認定後個人情報に署名をつけて保証する
→ IDCを持っていれば正当な仕組みで
本人認証がされていることを保証できる
→ オフラインでの取引に有効
945
940
910
IDA
930
IDC
920
Device 1(User)
コンテンツ
UCP
価格情報
使用制御情報
Device 2(User)
コンテンツ
UCP
価格情報
使用制御情報

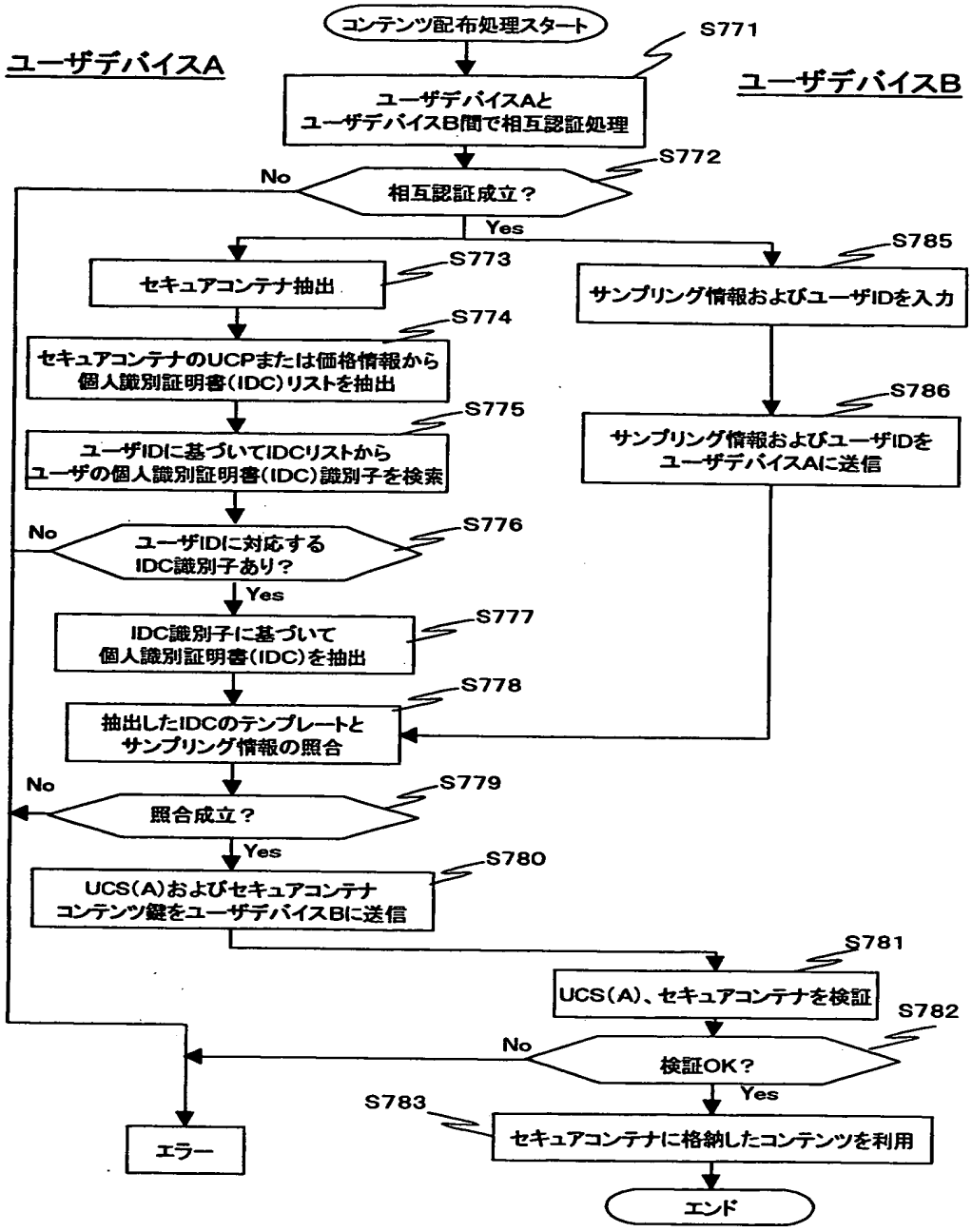
【図４３】


IDA
970
登録
User's Template
A
B
C
IDC
IDC配布
Device1での利用
Device2での利用
960
965
955
デバイス使用制限
使用制御情報(UCS)
コンテンツID
"A"
...
セキュアコンテナ
990
950
992
コンテンツ
UCP
価格情報
コンテンツ(セキュアコンテナ)のMove
Device 1(User)
Device 2(User)

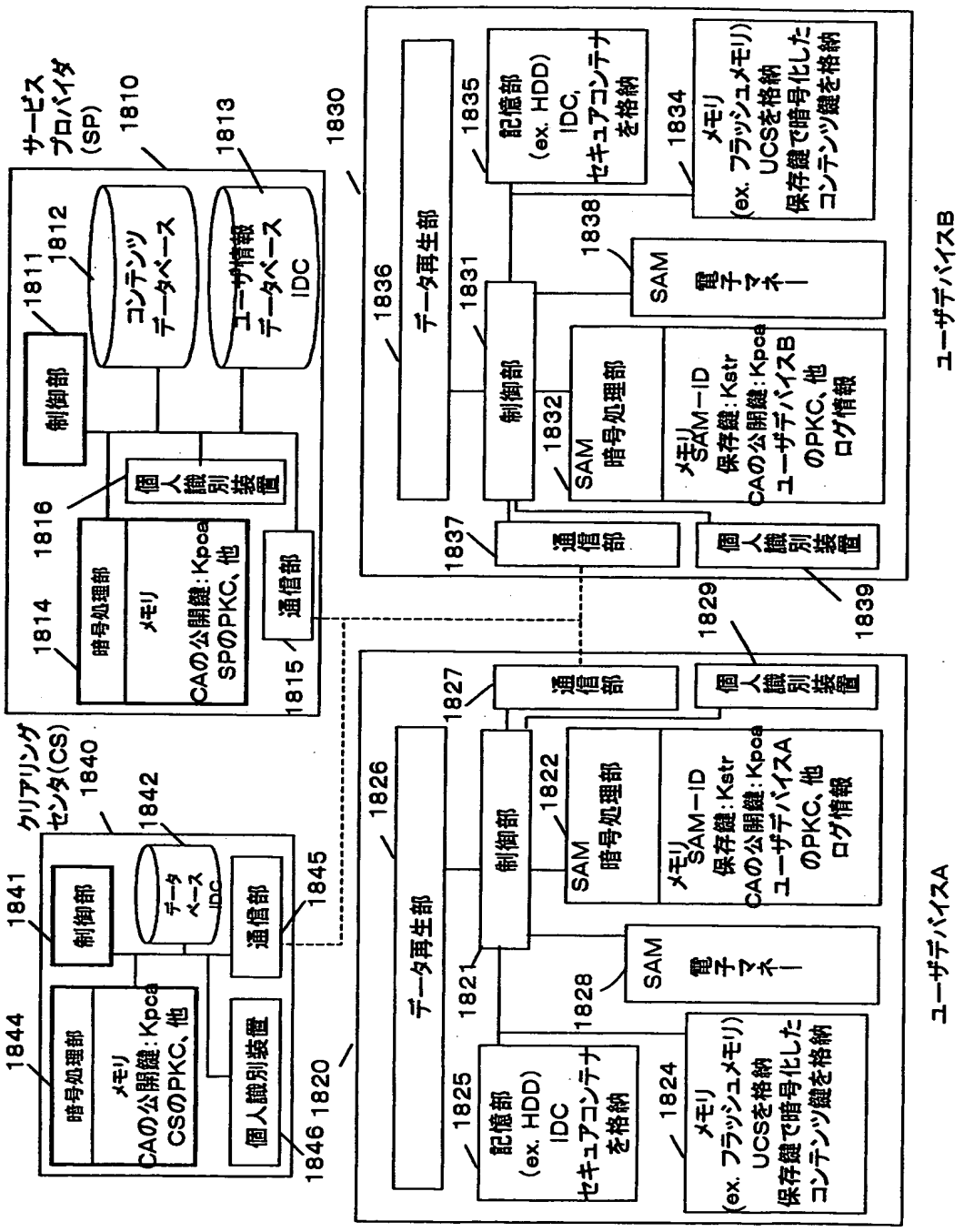
【図４４】


ユーザデバイスA
ユーザデバイスB
コンテンツ配布処理スタート
S751
ユーザデバイスAと
ユーザデバイスB間で相互認証処理
S752
No
相互認証成立？
Yes
セキュアコンテナ抽出
S753
セキュアコンテナをユーザデバイスBに送信
S754
S755
セキュアコンテナを検証
S756
No
セキュアコンテナの検証OK？
Yes
S757
サンプリング情報およびユーザIDを入力
S758
使用制御情報UCS(A)から
個人識別証明書(IDC)リストを抽出
S759
ユーザIDに基づいてIDCリストから
ユーザの個人識別証明書(IDC)識別子を検索
S760
No
ユーザIDに対応する
IDC識別子あり？
Yes
S761
IDC識別子に基づいて
個人識別証明書(IDC)を抽出
S762
抽出したIDCのテンプレートと
サンプリング情報の照合
S763
No
照合成立？
S764
照合成立を条件として
コンテンツ鍵送信
Yes
S765
セキュアコンテナに格納したコンテンツを利用
エラー
エンド

【図４５】

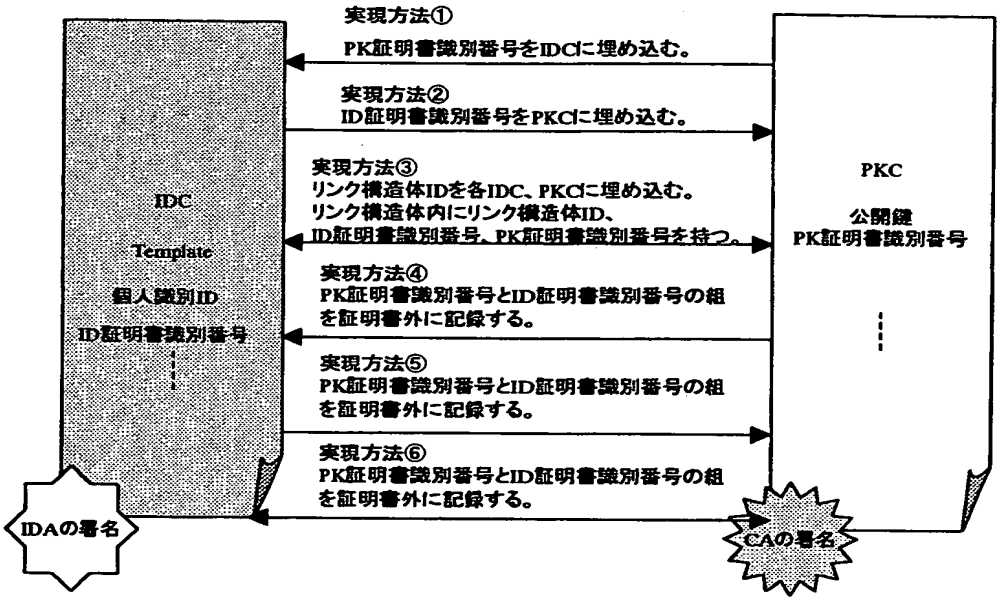

コンテンツ配布処理スタート
S771
ユーザデバイスA
ユーザデバイスB
ユーザデバイスAと
ユーザデバイスB間で相互認証処理
S772
No
相互認証成立？
Yes
S785
S773
セキュアコンテナ抽出
サンプリング情報およびユーザIDを入力
S774
セキュアコンテナのUCPまたは価格情報から
個人識別証明書(IDC)リストを抽出
S786
S775
ユーザIDに基づいてIDCリストから
ユーザの個人識別証明書(IDC)識別子を検索
サンプリング情報およびユーザIDを
ユーザデバイスAに送信
No
S776
ユーザIDに対応する
IDC識別子あり？
Yes
S777
IDC識別子に基づいて
個人識別証明書(IDC)を抽出
S778
抽出したIDCのテンプレートと
サンプリング情報の照合
No
S779
照合成立？
Yes
S780
UCS(A)およびセキュアコンテナ
コンテンツ鍵をユーザデバイスBに送信
S781
UCS(A)、セキュアコンテナを検証
S782
No
検証OK？
Yes
S783
エラー
セキュアコンテナに格納したコンテンツを利用
エンド

【図４６】

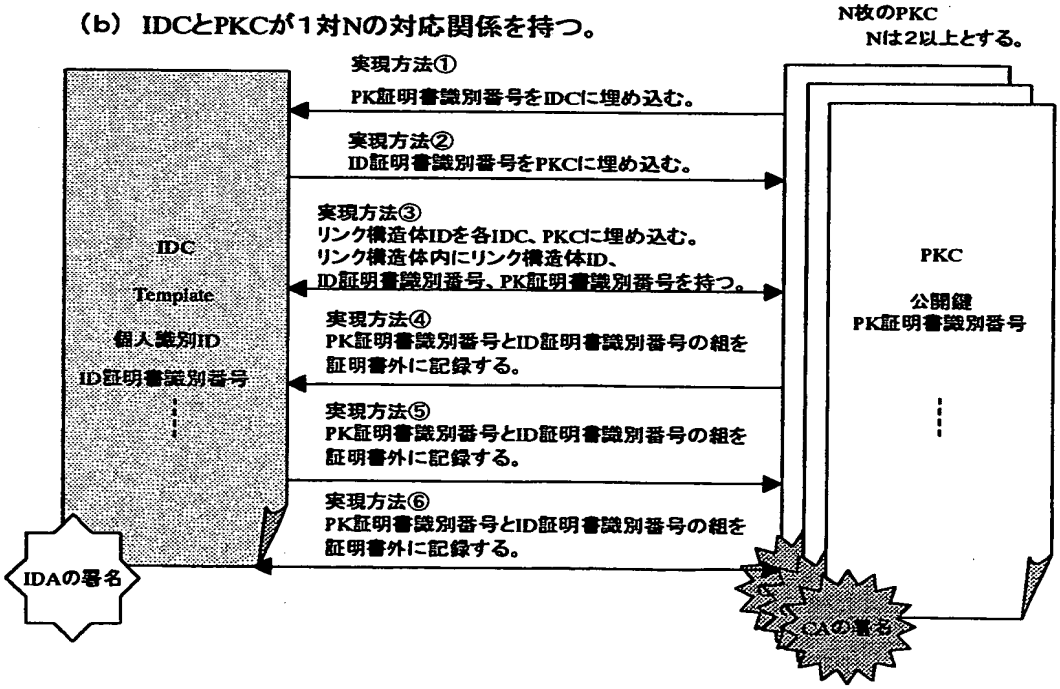

サービス
プロバイダ
(SP)
1810
1813
1830
1811
1812
制御部
コンテンツ
データベース
ユーザ情報
データベース
IDC
個人識別装置
1816
暗号処理部
メモリ
CAの公開鍵：Kpca
SPのPKC、他
通信部
1814
1815
クリアリング
センタ(CS)
1840
1842
1841
制御部
データ
ベース
IDC
通信部
1845
1844
暗号処理部
メモリ
CAの公開鍵：Kpca
CSのPKC、他
個人識別装置
1846
1820
ユーザデバイスA
1826
データ再生部
1827
通信部
個人識別装置
1829
1822
制御部
SAM
暗号処理部
メモリ
SAM−ID
保存鍵：Kstr
CAの公開鍵：Kpca
ユーザデバイスA
のPKC、他
ログ情報
1821
1828
SAM
電子マネー
1825
記憶部
(ex. HDD)
IDC
セキュアコンテナ
を格納
1824
メモリ
(ex. フラッシュメモリ)
UCSを格納
保存鍵で暗号化した
コンテンツ鍵を格納
ユーザデバイスB
1836
データ再生部
1835
記憶部
(ex. HDD)
IDC,
セキュアコンテナ
を格納
1834
メモリ
(ex. フラッシュメモリ)
UCSを格納
保存鍵で暗号化した
コンテンツ鍵を格納
1838
SAM
電子マネー
1831
制御部
1832
SAM
暗号処理部
メモリ
SAM−ID
保存鍵：Kstr
CAの公開鍵：Kpca
ユーザデバイスB
のPKC、他
ログ情報
1837
通信部
個人識別装置
1839

【図４７】

（a） IDCとPKCが1対1の対応関係を持つ。

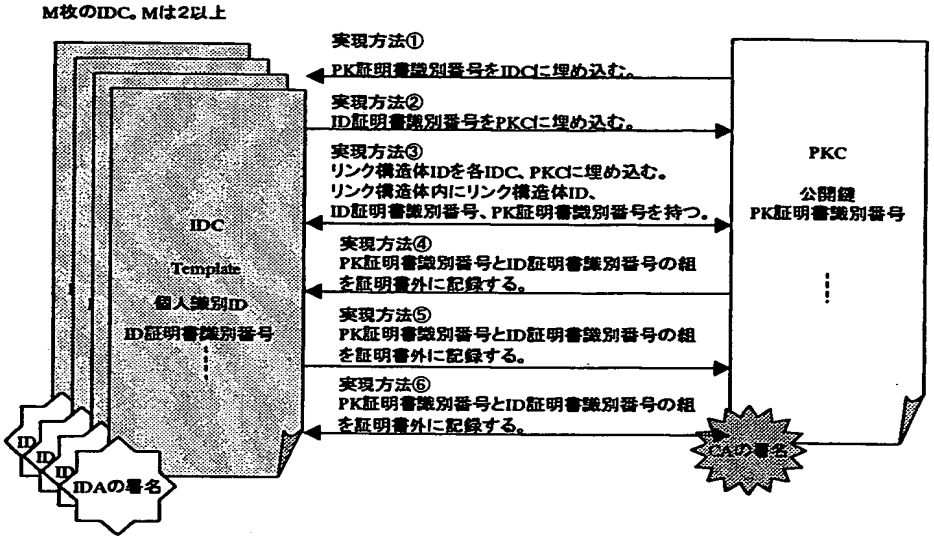


（b） IDCとPKCが1対Nの対応関係を持つ。

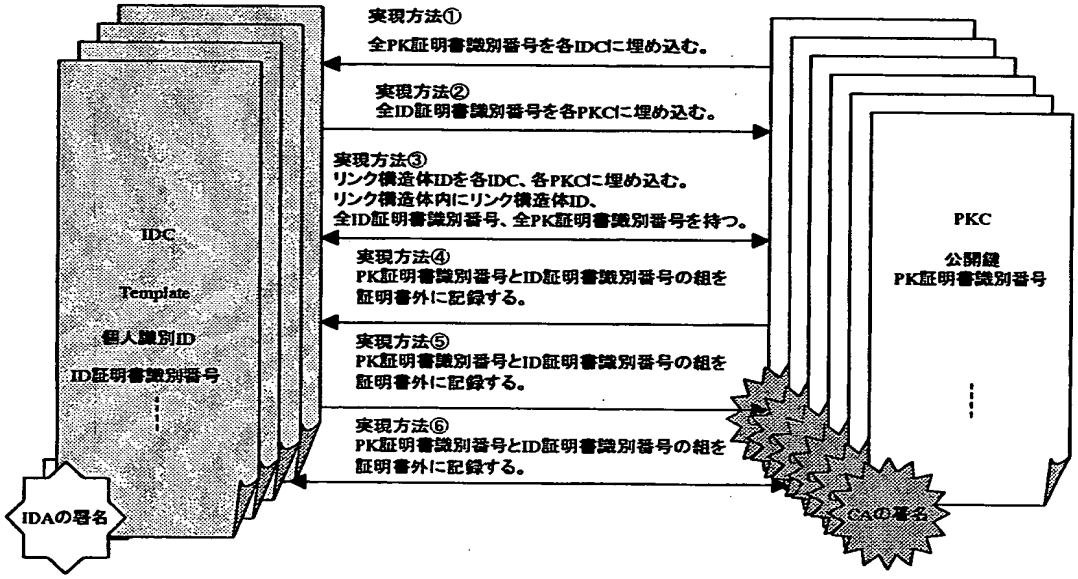


【図４８】

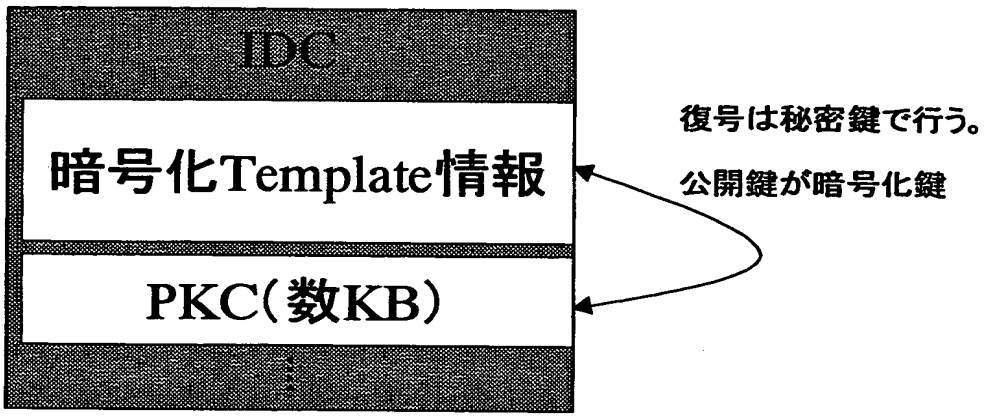
（c） IDCとPKCがM対1の対応関係を持つ。



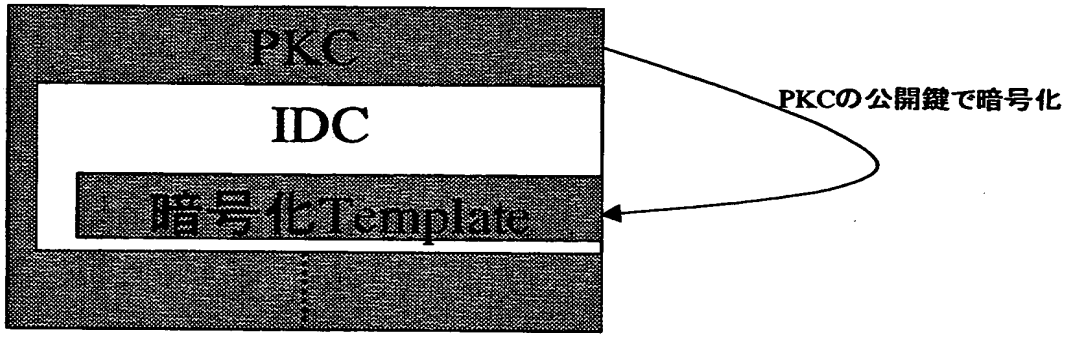
（d） IDCとPKCがM対Nの対応関係を持つ。



【図４９】

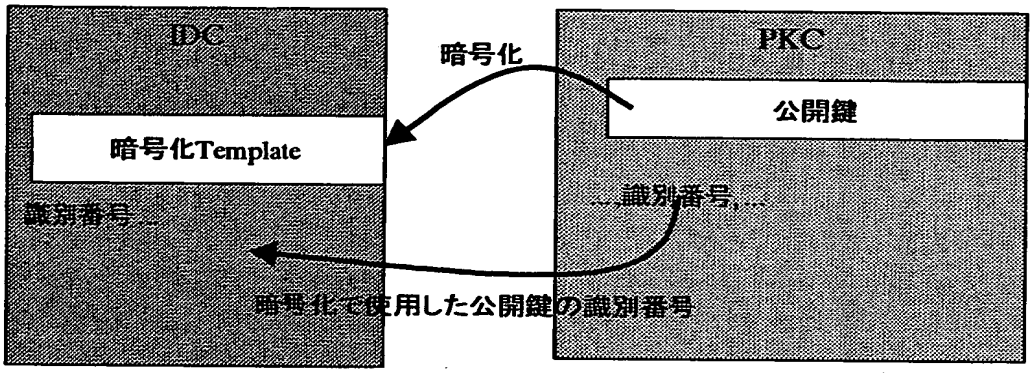

IDC
暗号化Template情報
PKC(数KB)
復号は秘密鍵で行う。
公開鍵が暗号化鍵

(a)

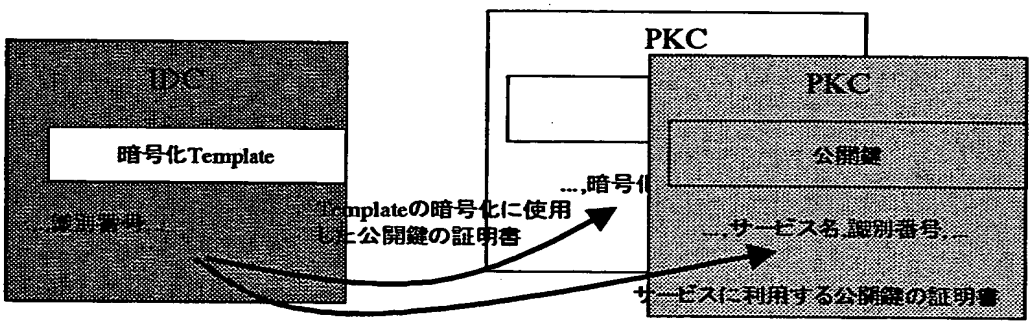

PKC
IDC
暗号化Template
PKCの公開鍵で暗号化

(b)

【図５０】

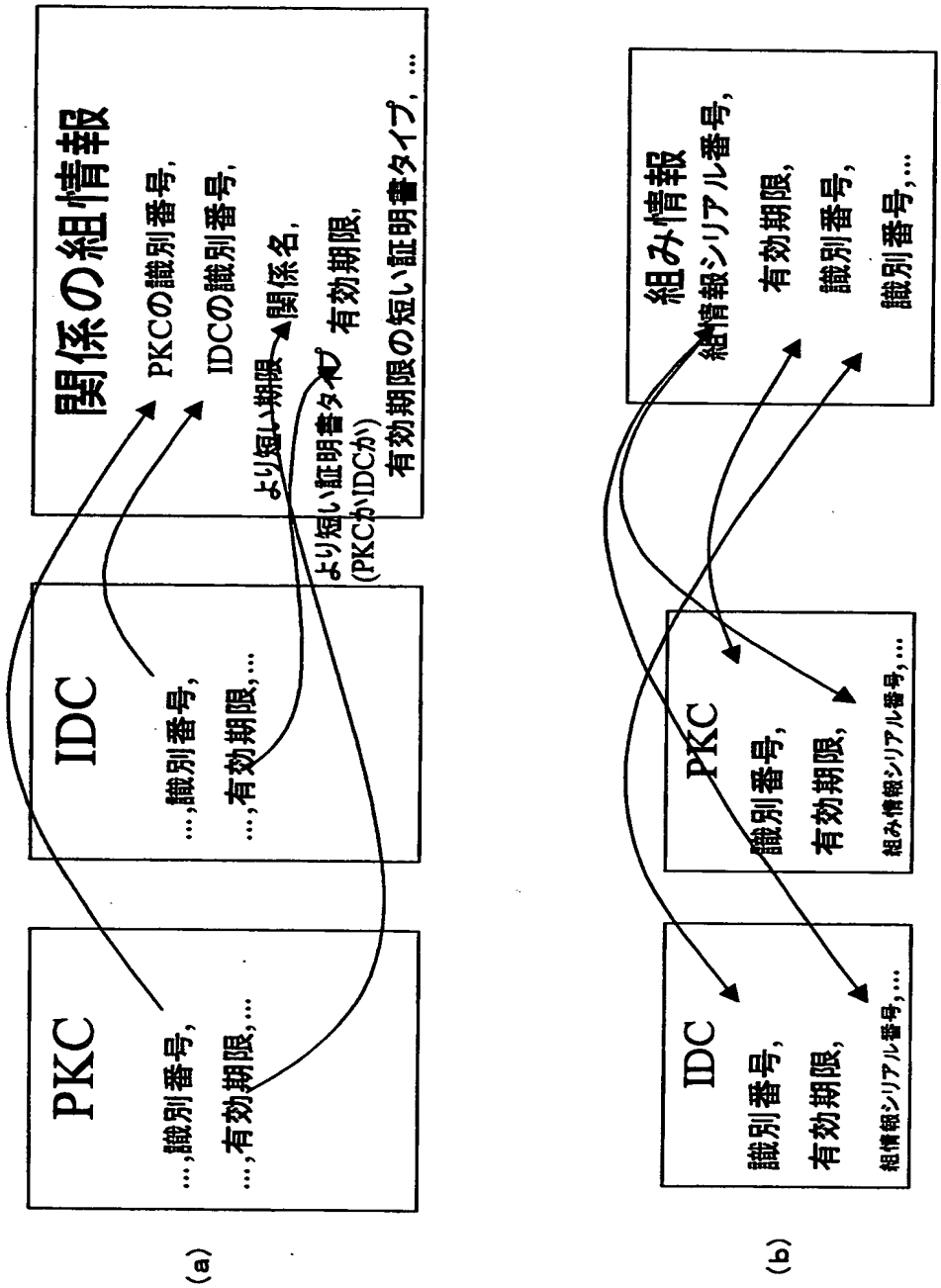

IDC
暗号化
PKC
公開鍵
暗号化Template
識別番号
識別番号
暗号化で使用した公開鍵の識別番号

(a)

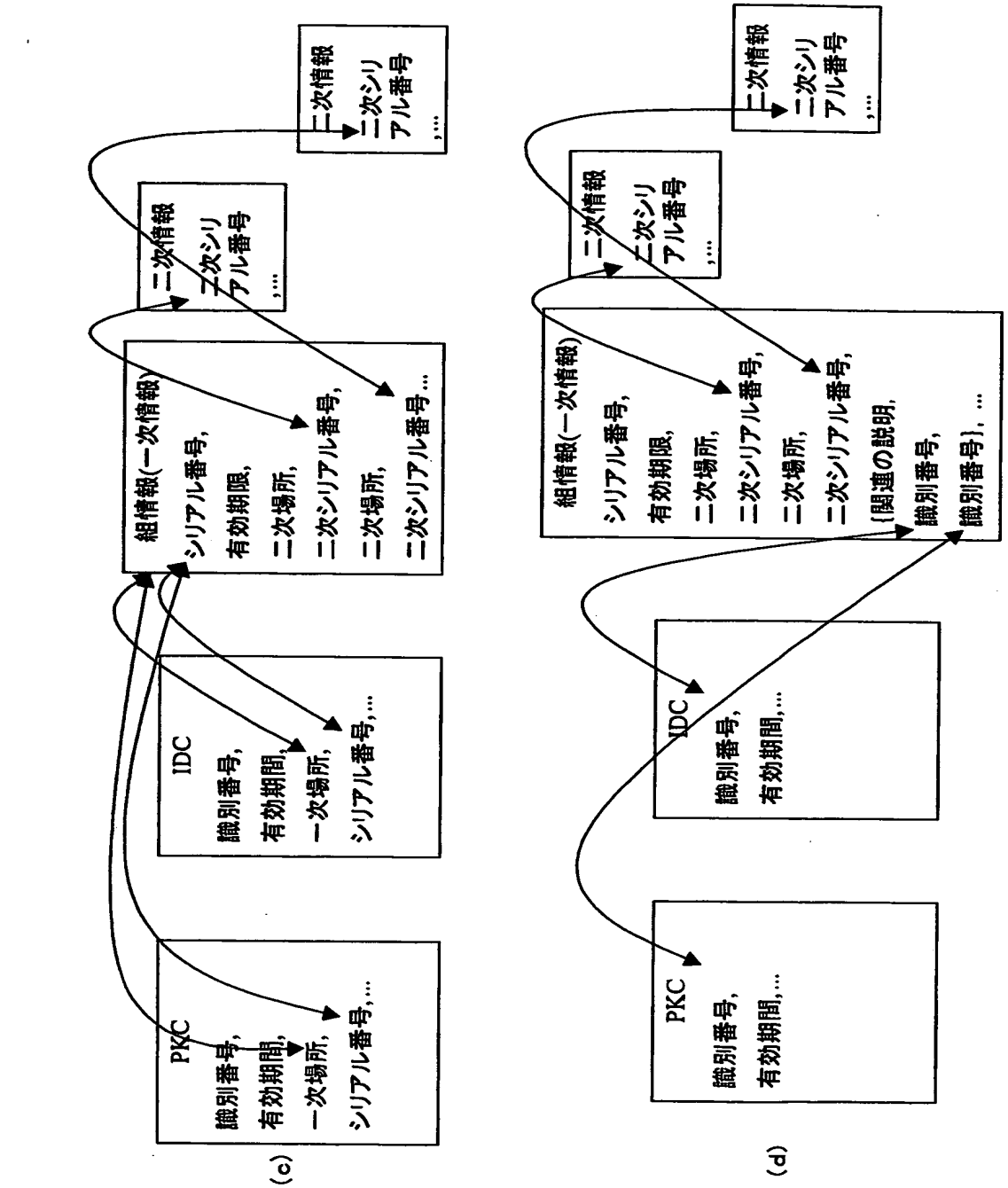

PKC
IDC
PKC
暗号化Template
公開鍵
Templateの暗号化に使用
した公開鍵の証明書
サービス名,識別番号
サービスに利用する公開鍵の証明書

(b)

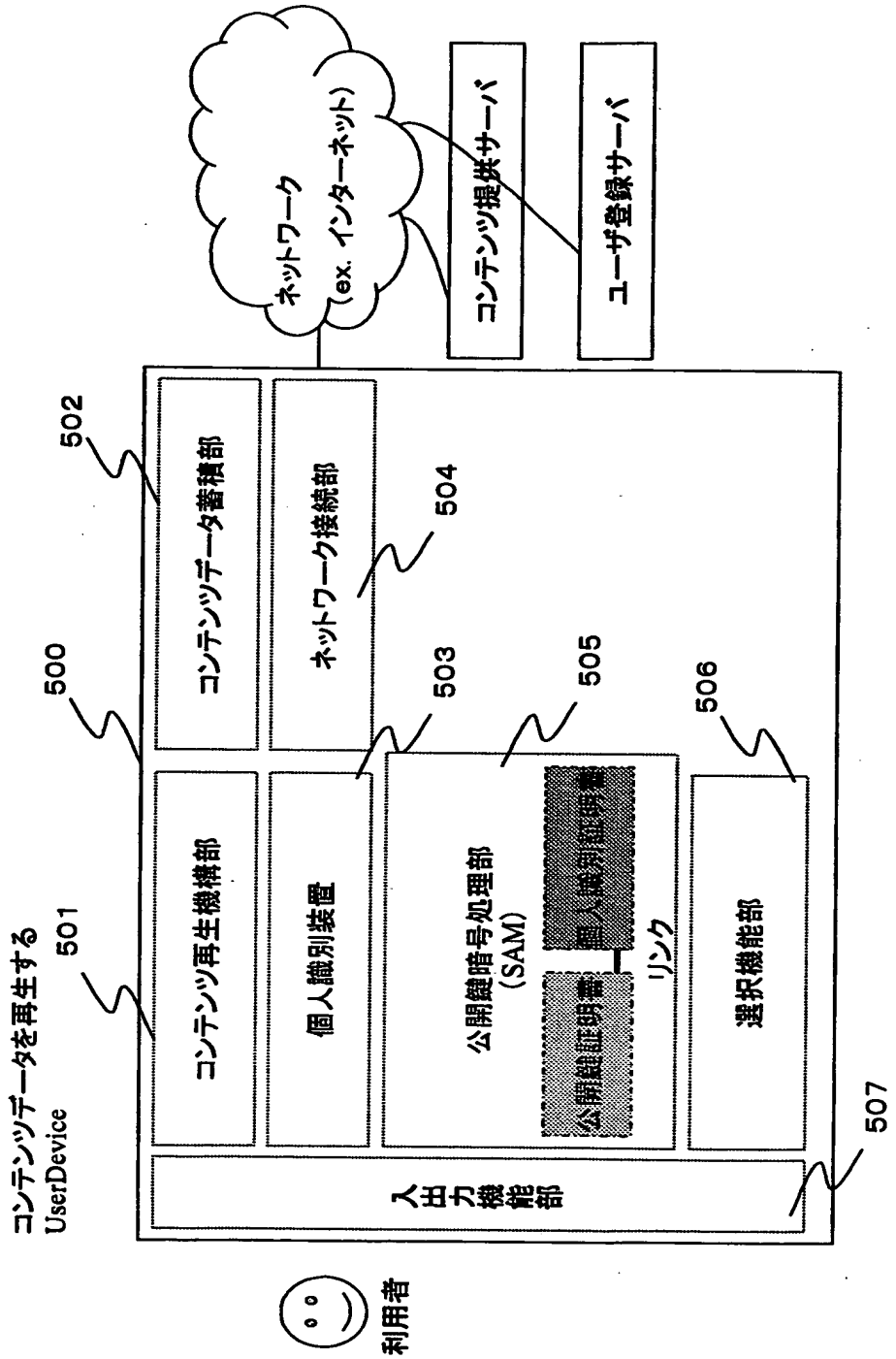
【図５１】


PKC
…,識別番号,
…,有効期限,…
IDC
…,識別番号,
…,有効期限,…
より短い期限→関係名,
より短い証明書タイプ
(PKCかIDCか)
有効期限,
有効期限の短い証明書タイプ,…
関係の組情報
PKCの識別番号,
IDCの識別番号,
(a)
PKC
識別番号,
有効期限,
組み情報シリアル番号,…
IDC
識別番号,
有効期限,
組情報シリアル番号,…
組み情報
組情報シリアル番号,
有効期限,
識別番号,
識別番号,…
(b)

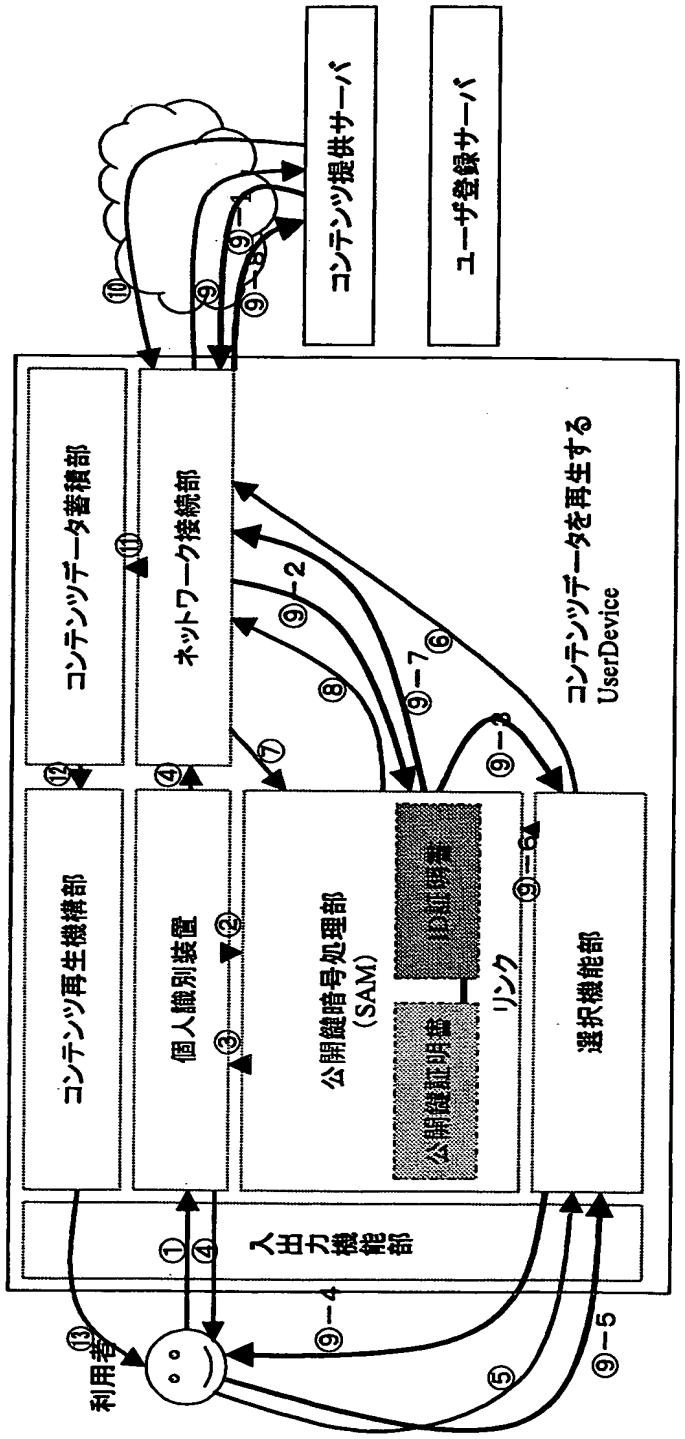
【図５２】


二次情報
二次シリアル番号,...
二次情報
二次シリアル番号,...
組情報(一次情報)
シリアル番号,
有効期限,
二次場所,
二次シリアル番号,
二次場所,
二次シリアル番号...
IDC
識別番号,
有効期間,
一次場所,
シリアル番号,...
PKC
識別番号,
有効期間,
一次場所,
シリアル番号,...
(c)
二次情報
二次シリアル番号,...
二次情報
二次シリアル番号,...
組情報(一次情報)
シリアル番号,
有効期限,
二次場所,
二次シリアル番号,
二次場所,
二次シリアル番号,
{関連の説明,
識別番号,
識別番号}, ...
IDC
識別番号,
有効期間,...
PKC
識別番号,
有効期間,...
(d)

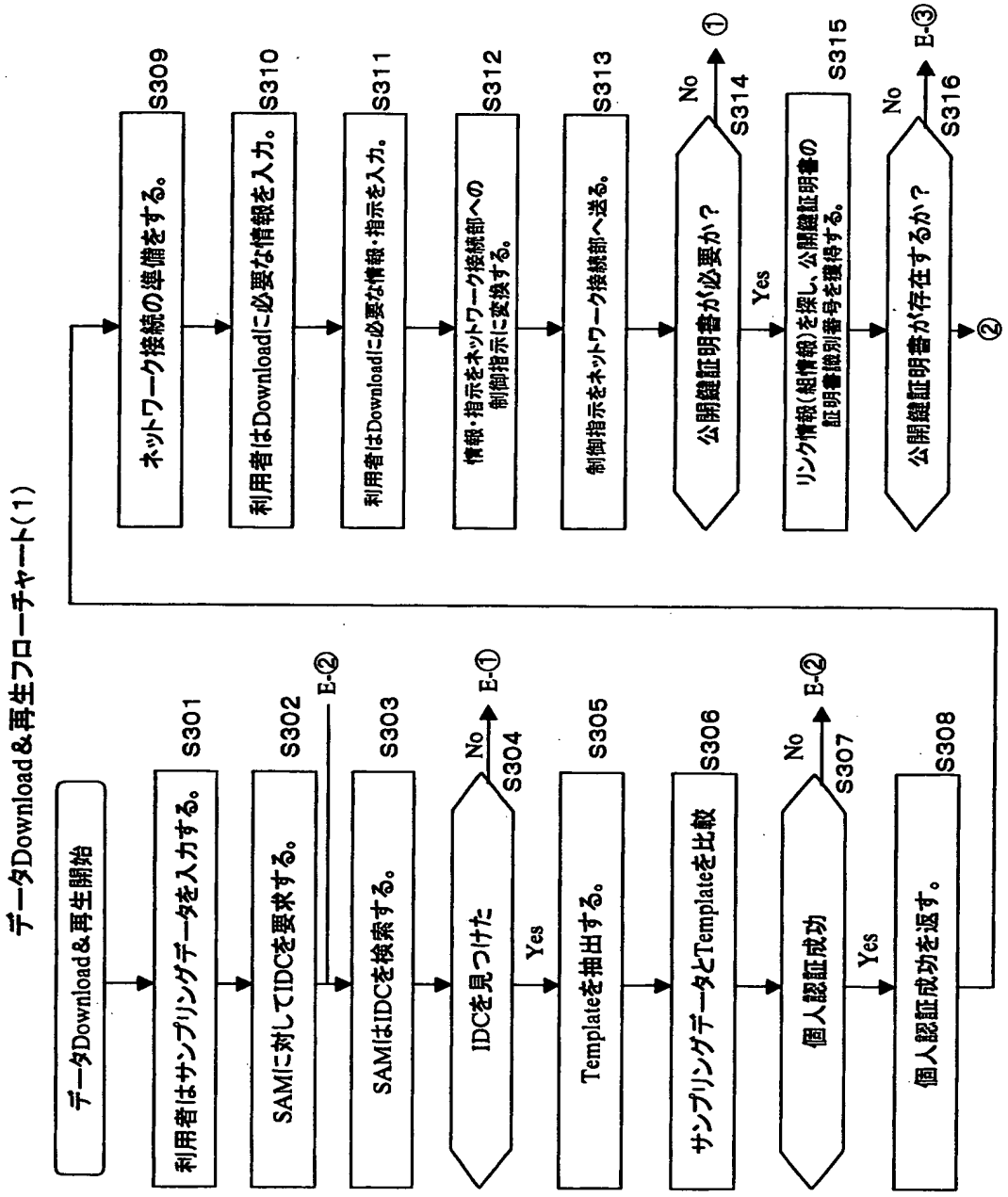
【図５３】


ネットワーク
(ex. インターネット)
コンテンツ提供サーバ
ユーザ登録サーバ
502
504
500
503
505
506
コンテンツデータ蓄積部
ネットワーク接続部
コンテンツ再生機構部
個人識別装置
公開鍵暗号処理部
(SAM)
公開鍵証明書
個人識別証明書
リンク
選択機能部
501
507
入出力機能部
コンテンツデータを再生する
UserDevice
利用者

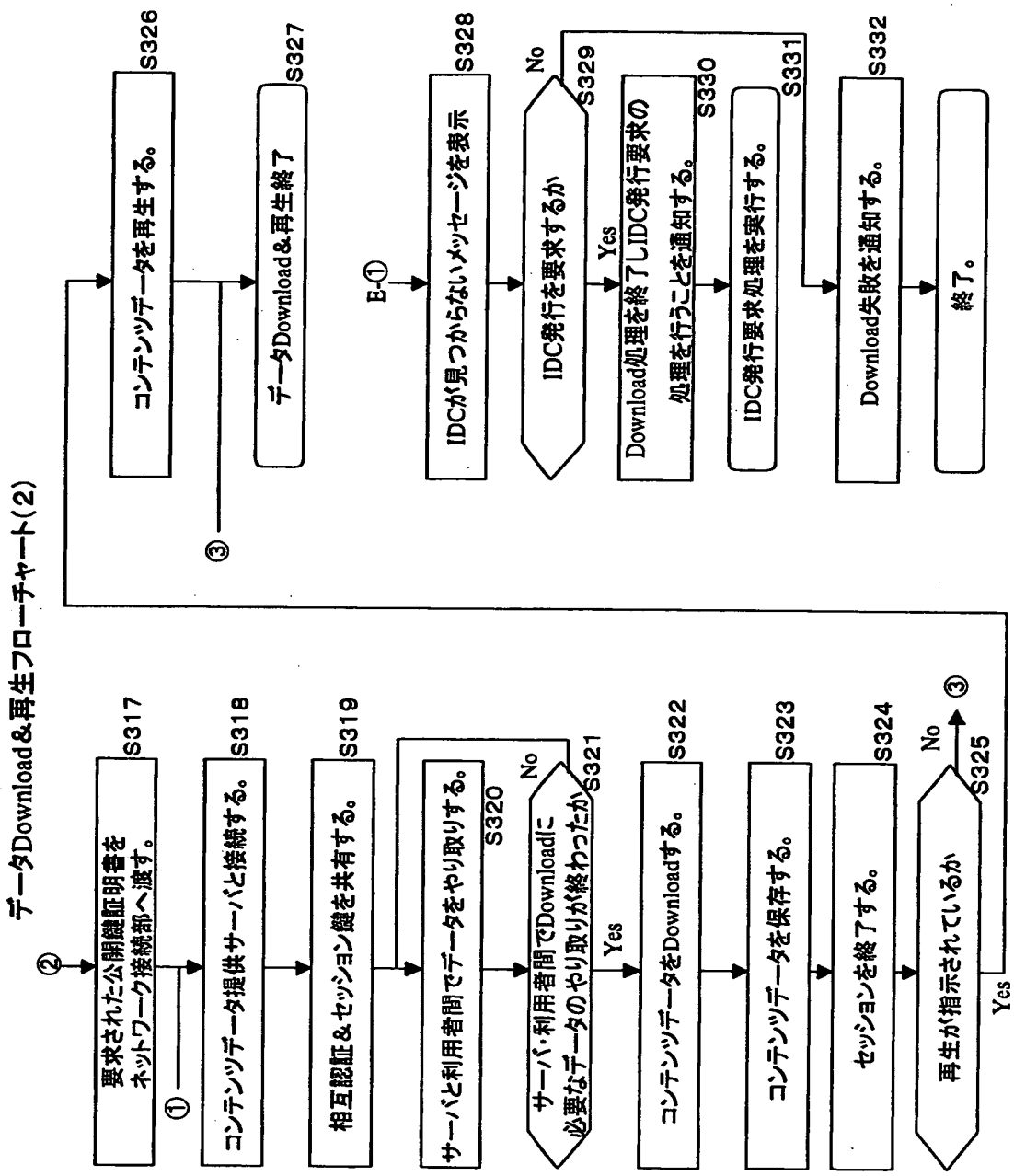
【図５４】


データDownload&再生
前提条件:
既にIDCとPKCを獲得している。
コンテンツ提供サーバに対して必要なユーザ登録は終えている。
コンテンツ提供サーバ
ユーザ登録サーバ
コンテンツデータ蓄積部
ネットワーク接続部
コンテンツデータを再生する
UserDevice
コンテンツ再生機構部
個人識別装置
公開鍵暗号処理部
(SAM)
ID証明書
公開鍵証明書
リンク
選択機能部
入出力機能部
利用者

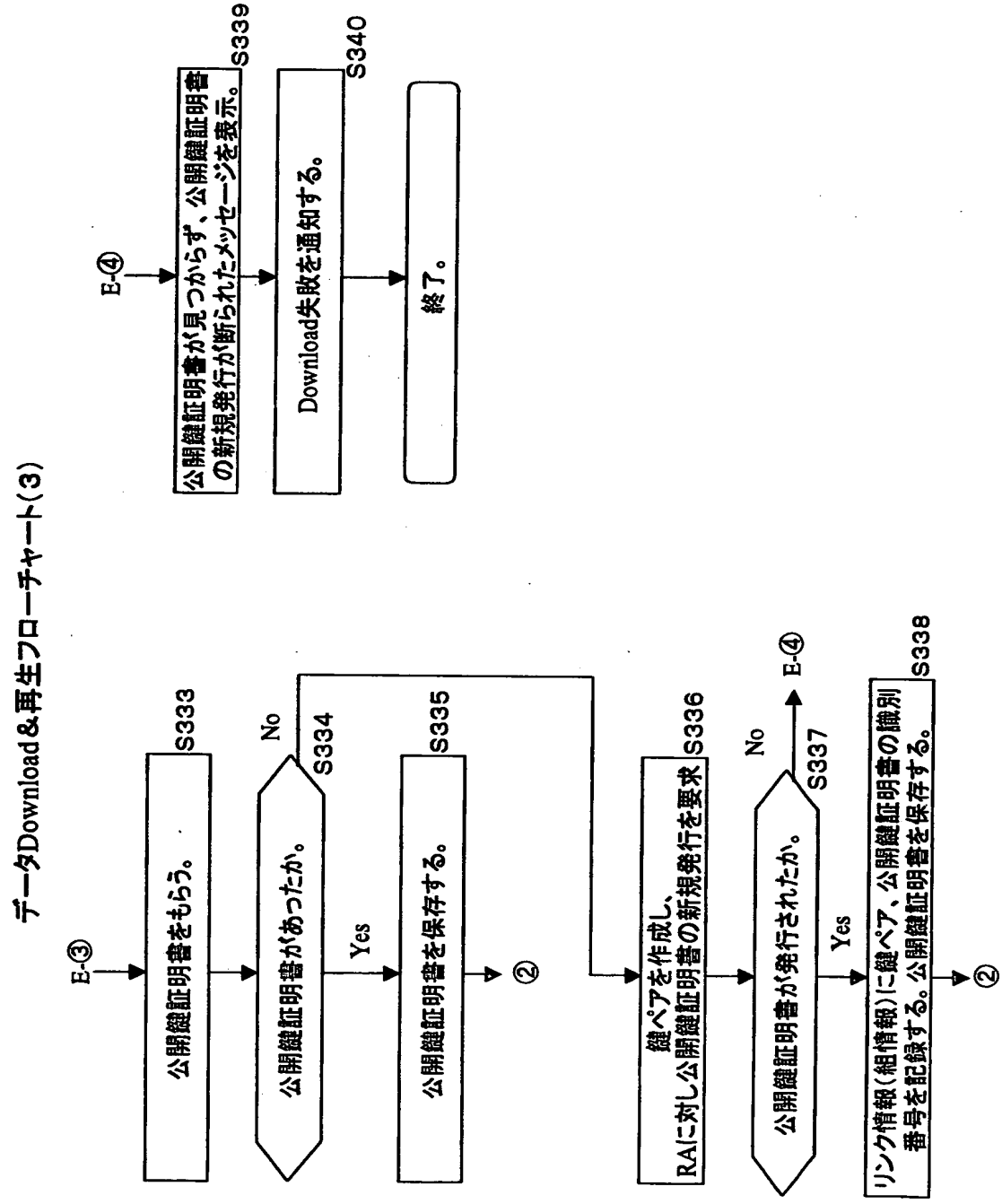
【図５５】


データDownload&再生フローチャート(1)
データDownload&再生開始
利用者はサンプリングデータを入力する。
S301
SAMに対してIDCを要求する。
S302
E-②
SAMはIDCを検索する。
S303
IDCを見つけた
No
S304
E-①
Yes
Templateを抽出する。
S305
サンプリングデータとTemplateを比較
S306
個人認証成功
No
S307
E-②
Yes
個人認証成功を返す。
S308
ネットワーク接続の準備をする。
S309
利用者はDownloadに必要な情報を入力。
S310
利用者はDownloadに必要な情報・指示を入力。
S311
情報・指示をネットワーク接続部への制御指示に変換する。
S312
制御指示をネットワーク接続部へ送る。
S313
公開鍵証明書が必要か？
No
S314
①
Yes
リンク情報(相情報)を探し、公開鍵証明書の証明書識別番号を獲得する。
S315
公開鍵証明書が存在するか？
No
S316
E-③
②

【図５６】


データDownload&再生フローチャート(2)
②
要求された公開鍵証明書をネットワーク接続部へ渡す。
S317
①
コンテンツデータ提供サーバと接続する。
S318
相互認証＆セッション鍵を共有する。
S319
サーバと利用者間でデータをやり取りする。
S320
サーバ・利用者間でDownloadに必要なデータのやり取りが終わったか
No
S321
Yes
コンテンツデータをDownloadする。
S322
コンテンツデータを保存する。
S323
セッションを終了する。
S324
再生が指示されているか
No
③
S325
Yes
コンテンツデータを再生する。
S326
③
データDownload&再生終了
S327
E-①
IDCが見つからないメッセージを表示
S328
IDC発行を要求するか
No
S329
Yes
Download処理を終了しIDC発行要求の処理を行うことを通知する。
S330
IDC発行要求処理を実行する。
S331
Downloadに失敗を通知する。
S332
終了。

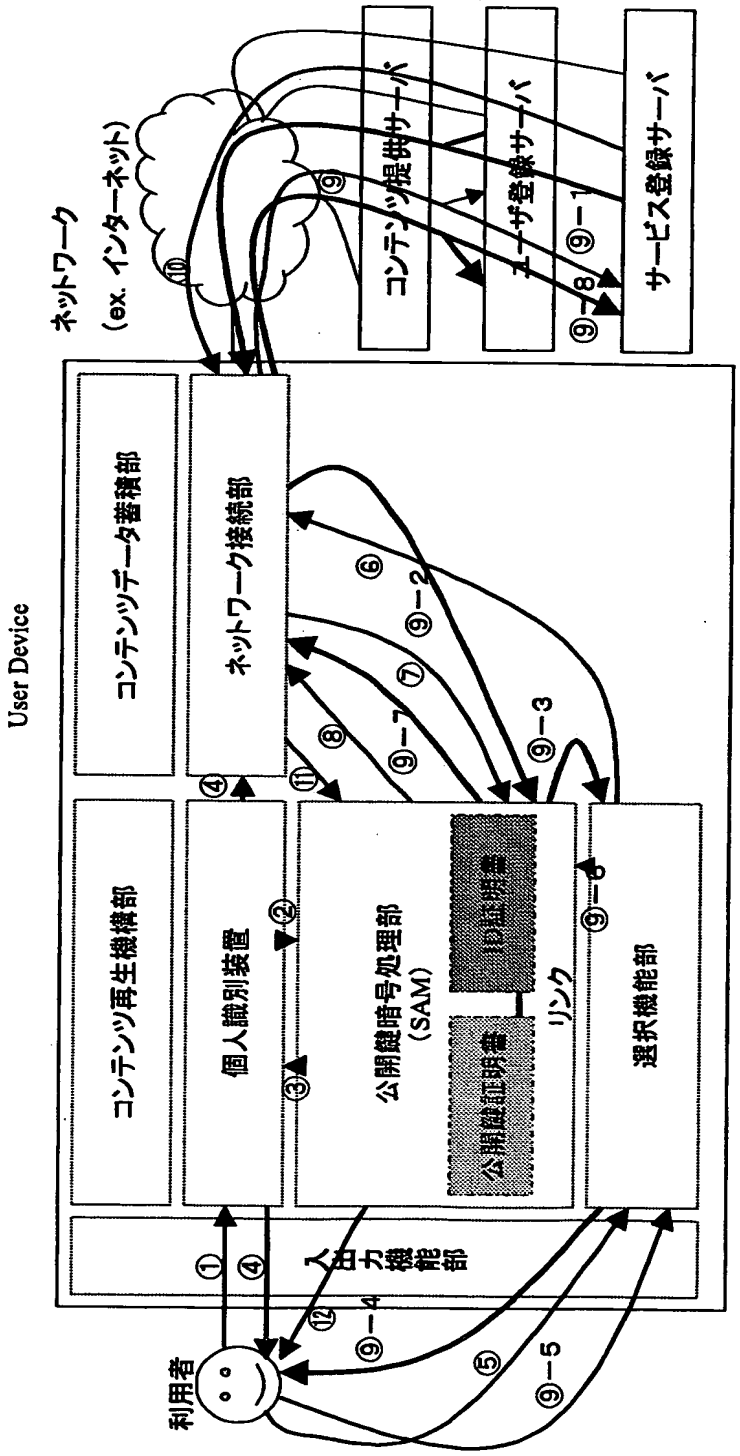
【図５７】


データDownload＆再生フローチャート(3)
E-③
公開鍵証明書をもらう。
S333
公開鍵証明書があったか。
No
S334
Yes
公開鍵証明書を保存する。
S335
②
鍵ペアを作成し、
RAに対し公開鍵証明書の新規発行を要求
S336
公開鍵証明書が発行されたか。
No
S337
E-④
Yes
リンク情報(組情報)に鍵ペア、公開鍵証明書の識別番号を記録する。公開鍵証明書を保存する。
S338
②
E-④
公開鍵証明書が見つからず、公開鍵証明書の新規発行が断られたメッセージを表示。
S339
Download失敗を通知する。
S340
終了。

【図５８】

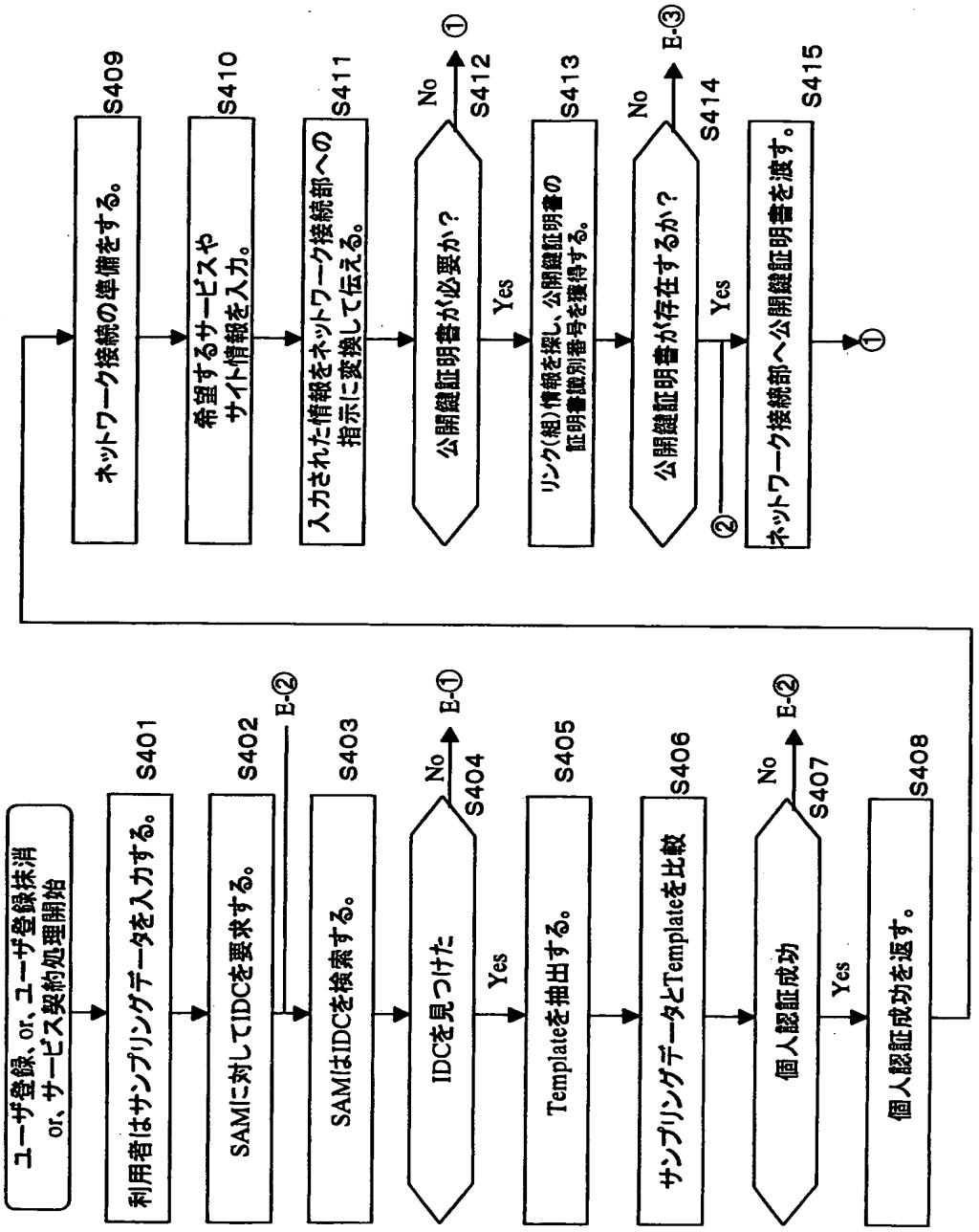
ユーザ登録、ユーザ登録抹消、サービス契約における処理の流れ

- 前提条件：
  - 既にIDCとPKCを獲得している。

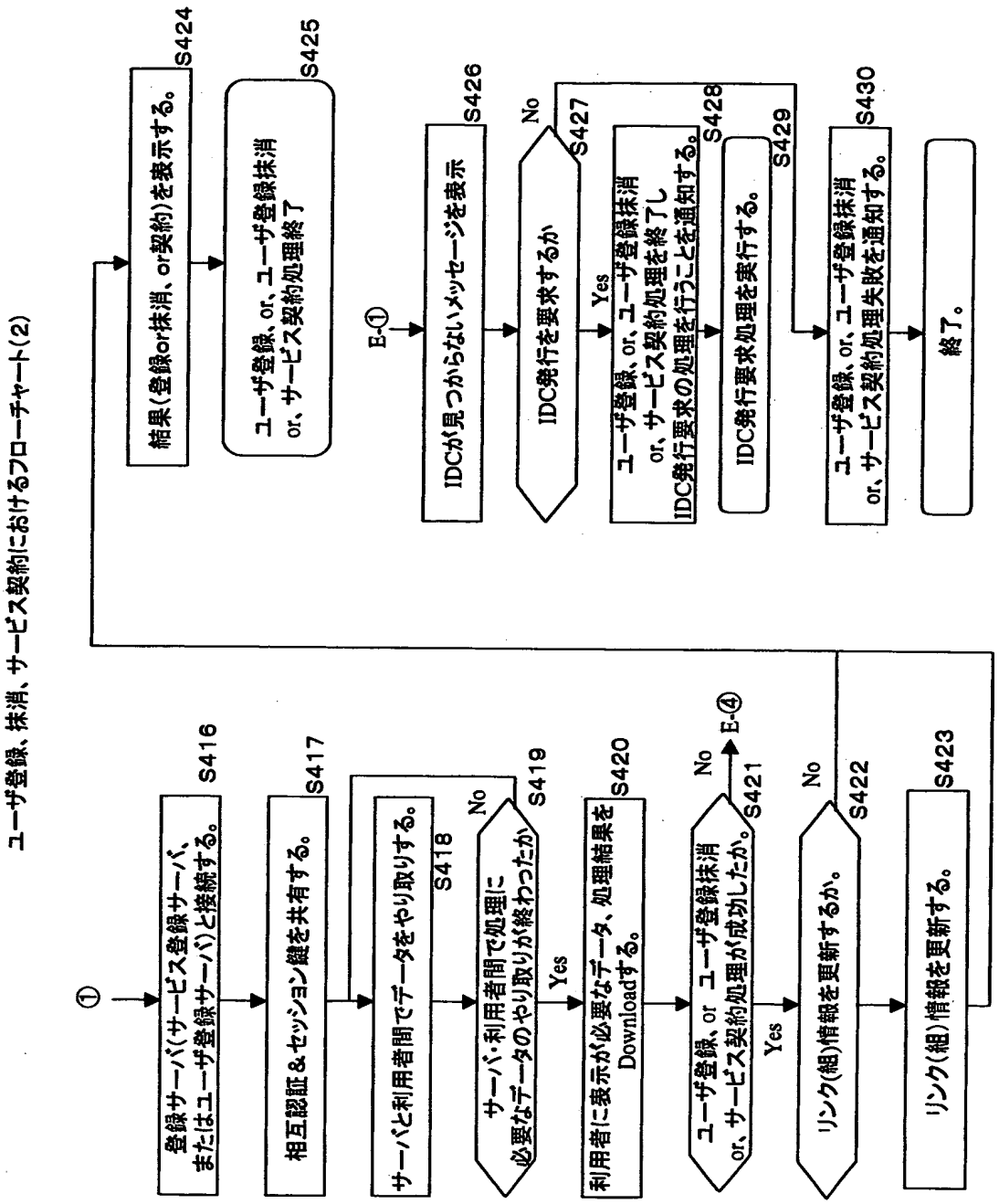


【図５９】

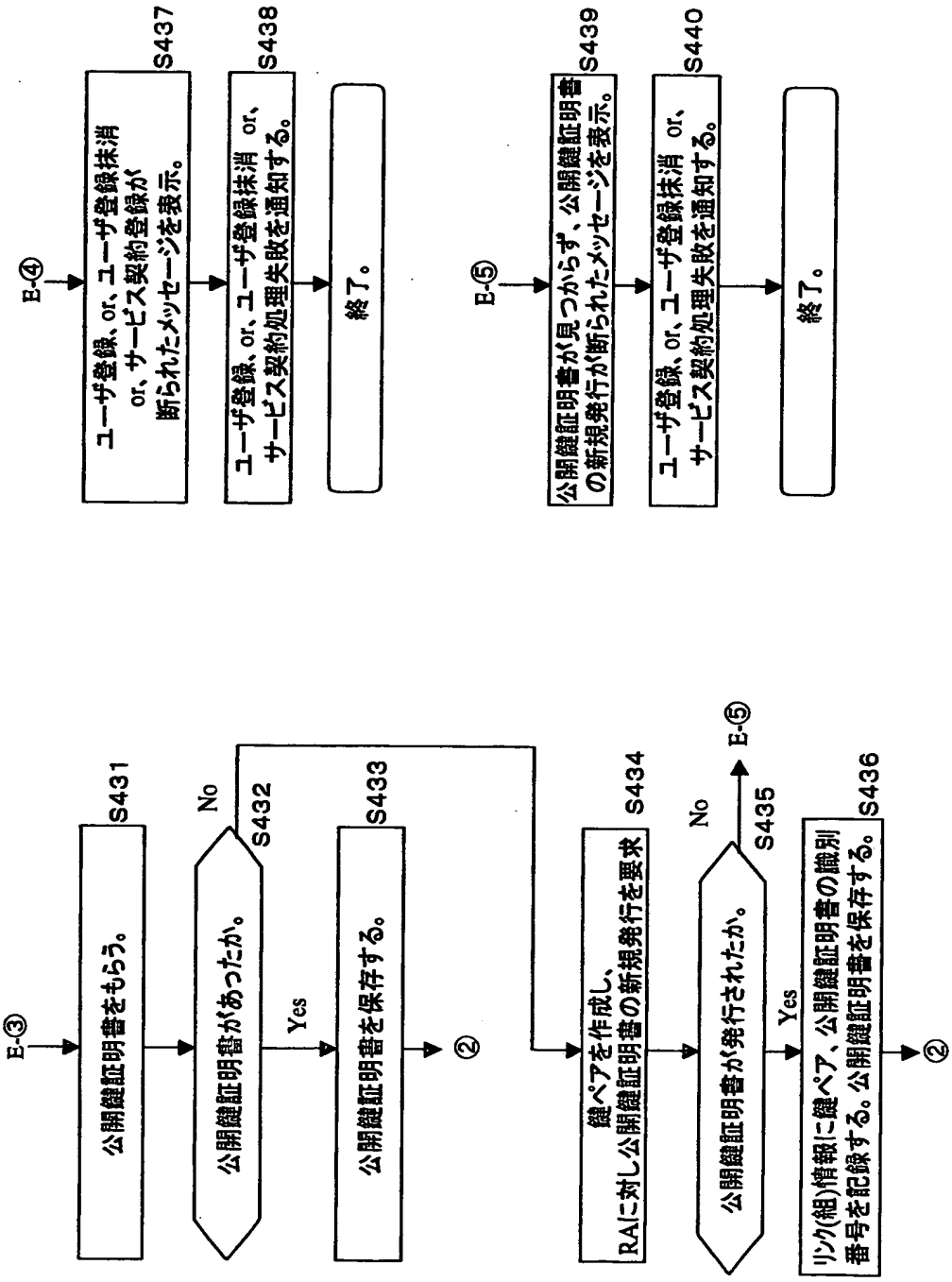
ユーザ登録、抹消、サービス契約におけるフローチャート(1)



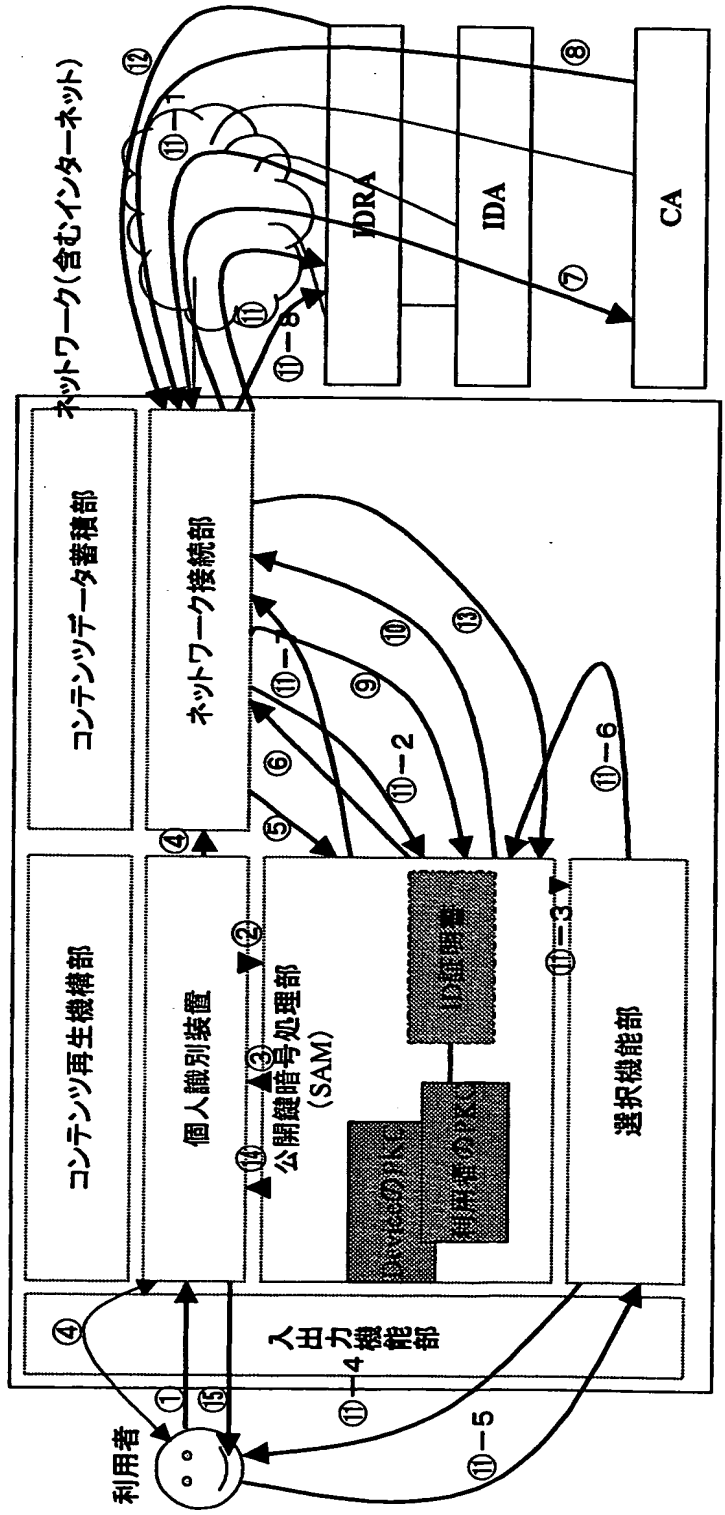
【図６０】


ユーザ登録、抹消、サービス契約におけるフローチャート(2)
①
登録サーバ(サービス登録サーバ、またはユーザ登録サーバ)と接続する。
S416
相互認証＆セッション鍵を共有する。
S417
サーバと利用者間でデータをやり取りする。
S418
サーバ・利用者間で処理に必要なデータのやり取りが終わったか
S419
No
Yes
利用者に表示が必要なデータ、処理結果をDownloadする。
S420
ユーザ登録、or ユーザ登録抹消or、サービス契約処理が成功したか。
S421
No
E-④
Yes
リンク(組)情報を更新するか。
S422
No
リンク(組)情報を更新する。
S423
結果(登録or抹消、or契約)を表示する。
S424
ユーザ登録、or、ユーザ登録抹消or、サービス契約処理終了
S425
E-①
IDCが見つからないメッセージを表示
S426
IDC発行を要求するか
S427
No
Yes
ユーザ登録、or、ユーザ登録抹消or、サービス契約処理を終了しIDC発行要求の処理を行うことを通知する。
S428
IDC発行要求処理を実行する。
S429
ユーザ登録、or、ユーザ登録抹消or、サービス契約処理失敗を通知する。
S430
終了。

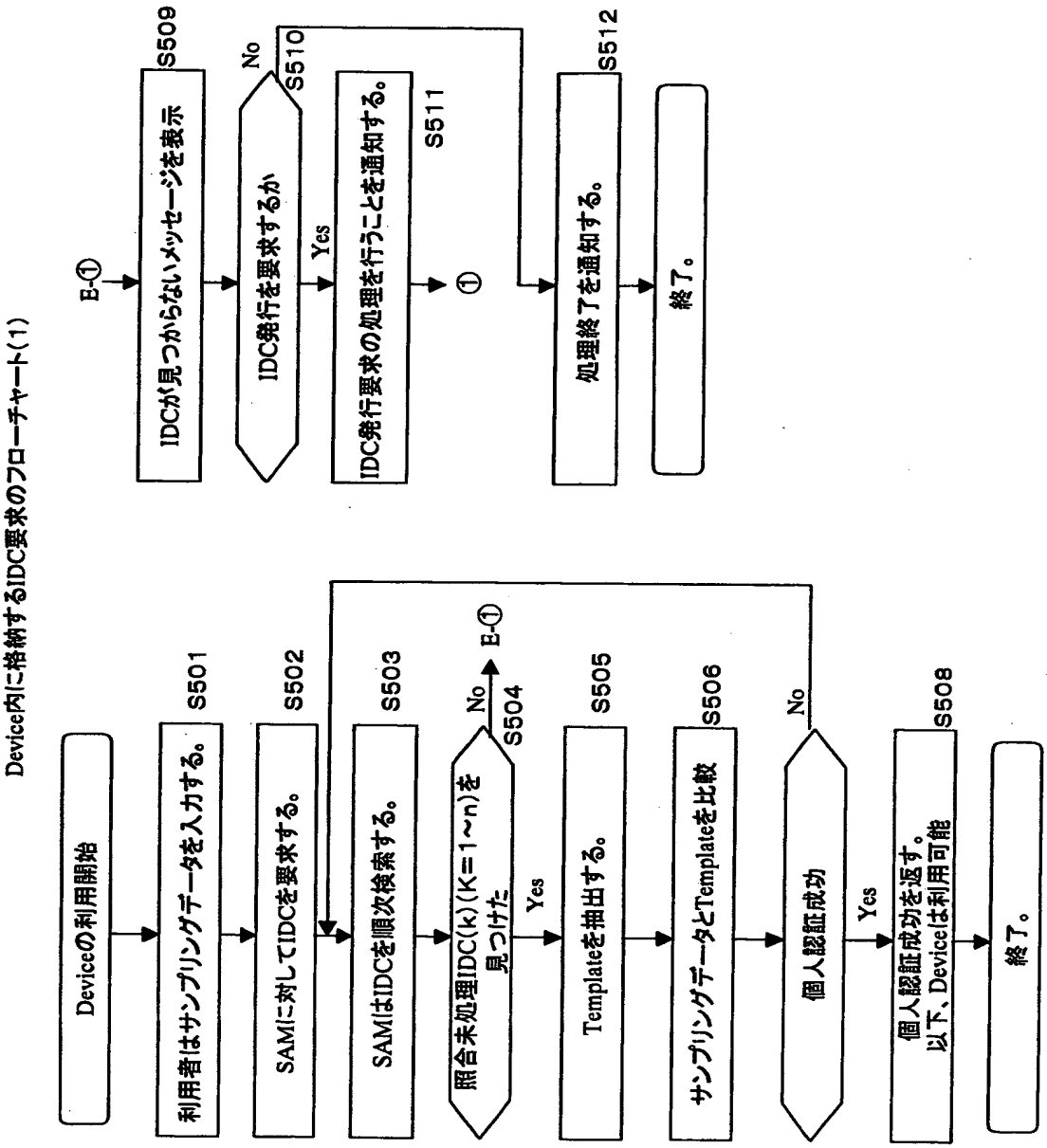
【図６１】


ユーザ登録、抹消、サービス契約におけるフローチャート(3)
E-③
公開鍵証明書をもらう。
S431
公開鍵証明書があったか。
No
S432
Yes
公開鍵証明書を保存する。
S433
②
鍵ペアを作成し、
RAに対し公開鍵証明書の新規発行を要求
S434
No
公開鍵証明書が発行されたか。
S435
E-⑤
Yes
リンク(組)情報に鍵ペア、公開鍵証明書の識別番号を記録する。公開鍵証明書を保存する。
S436
②
E-④
ユーザ登録、or、ユーザ登録抹消
or、サービス契約登録が
断られたメッセージを表示。
S437
ユーザ登録、or、ユーザ登録抹消 or、
サービス契約処理失敗を通知する。
S438
終了。
E-⑤
公開鍵証明書が見つからず、公開鍵証明書
の新規発行が断られたメッセージを表示。
S439
ユーザ登録、or、ユーザ登録抹消 or、
サービス契約処理失敗を通知する。
S440
終了。

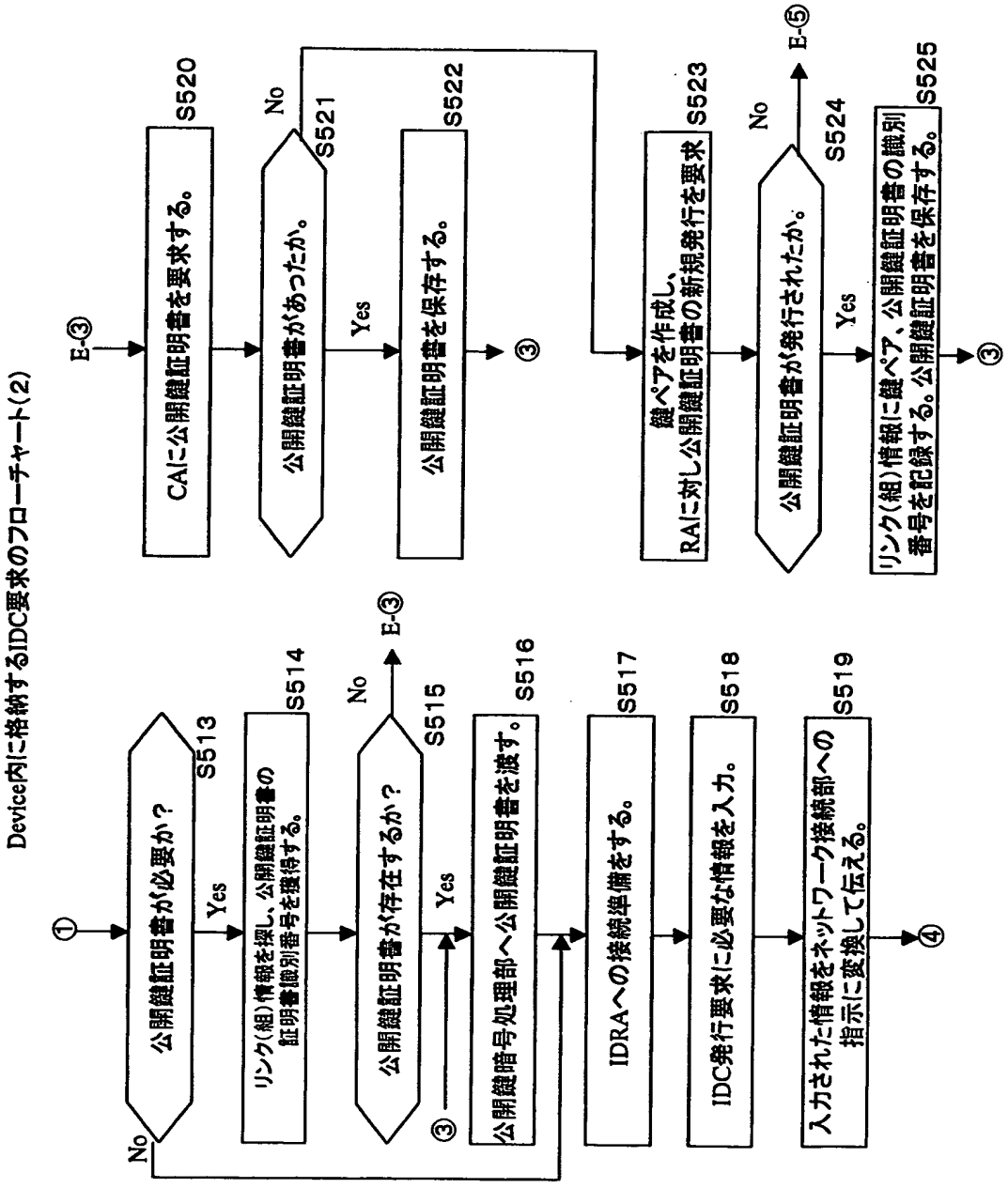
【図６２】


Device内に格納するIDCの要求
• 前提条件:
– UserDeviceはIDCを未登録で、かつ、Templateを保有していない。
– UserDeviceはPKCを未保持。鍵ペアを保有していないが、生成可能。
– IDC発行に必要なOffline手続きは済ませてあることと、その際、申込者とTemplate提供者の一致を確認するための情報(PIN or Templateそのもの or 秘密鍵による署名など)を設定し決定しているものとする。
コンテンツを再生するUserDevice
ネットワーク(含むインターネット)
コンテンツ再生機構部
コンテンツデータ蓄積部
個人識別装置
ネットワーク接続部
公開鍵暗号処理部
(SAM)
IDRA
IDA
CA
ID証明書
利用者のPKC
Deviceの PKC
入出力機能部
選択機能部
利用者

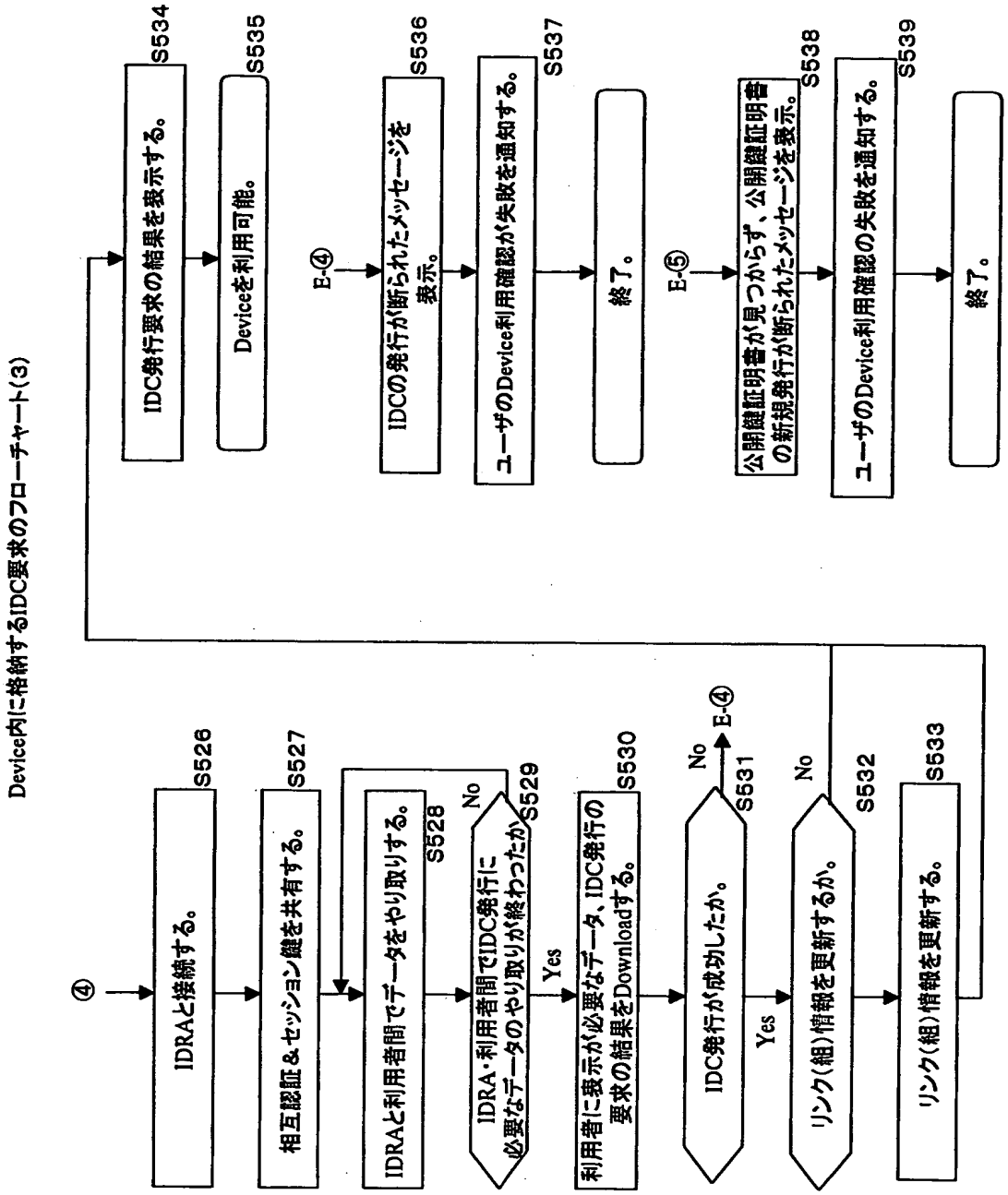
【図６３】


Device内に格納するIDC要求のフローチャート(1)
Deviceの利用開始
利用者はサンプリングデータを入力する。
S501
SAMに対してIDCを要求する。
S502
SAMはIDCを順次検索する。
S503
照合未処理IDC(k)(K=1～n)を見つけた
No
S504
Yes
E-①
Templateを抽出する。
S505
サンプリングデータとTemplateを比較
S506
個人認証成功
No
Yes
個人認証成功を返す。
以下、Deviceは利用可能
S508
終了。
E-①
IDCが見つからないメッセージを表示
S509
IDC発行を要求するか
No
S510
Yes
IDC発行要求の処理を行うことを通知する。
S511
①
処理終了を通知する。
S512
終了。

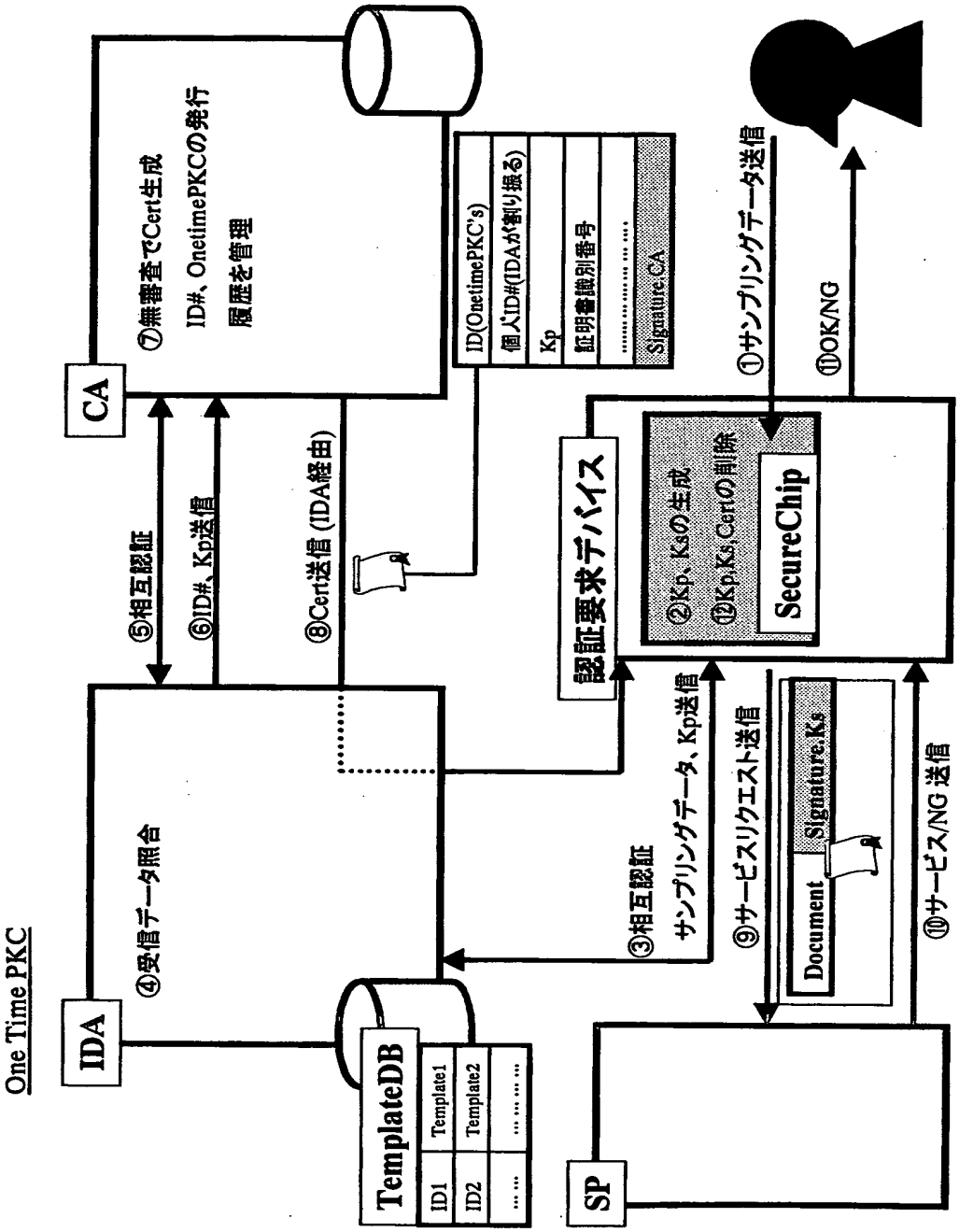
【図６４】


Device内に格納するIDC要求のフローチャート(2)
①
公開鍵証明書が必要か？
S513
Yes
No
リンク(組)情報を探し、公開鍵証明書の証明書識別番号を獲得する。
S514
公開鍵証明書が存在するか？
S515
No
Yes
E-③
③
公開鍵暗号処理部へ公開鍵証明書を渡す。
S516
IDRAへの接続準備をする。
S517
IDC発行要求に必要な情報を入力。
S518
入力された情報をネットワーク接続部への指示に変換して伝える。
S519
④
E-③
CAに公開鍵証明書を要求する。
S520
公開鍵証明書があったか。
S521
No
Yes
公開鍵証明書を保存する。
S522
③
鍵ペアを作成し、RAに対し公開鍵証明書の新規発行を要求
S523
公開鍵証明書が発行されたか。
S524
No
Yes
E-⑤
リンク(組)情報に鍵ペア、公開鍵証明書の識別番号を記録する。公開鍵証明書を保存する。
S525
③

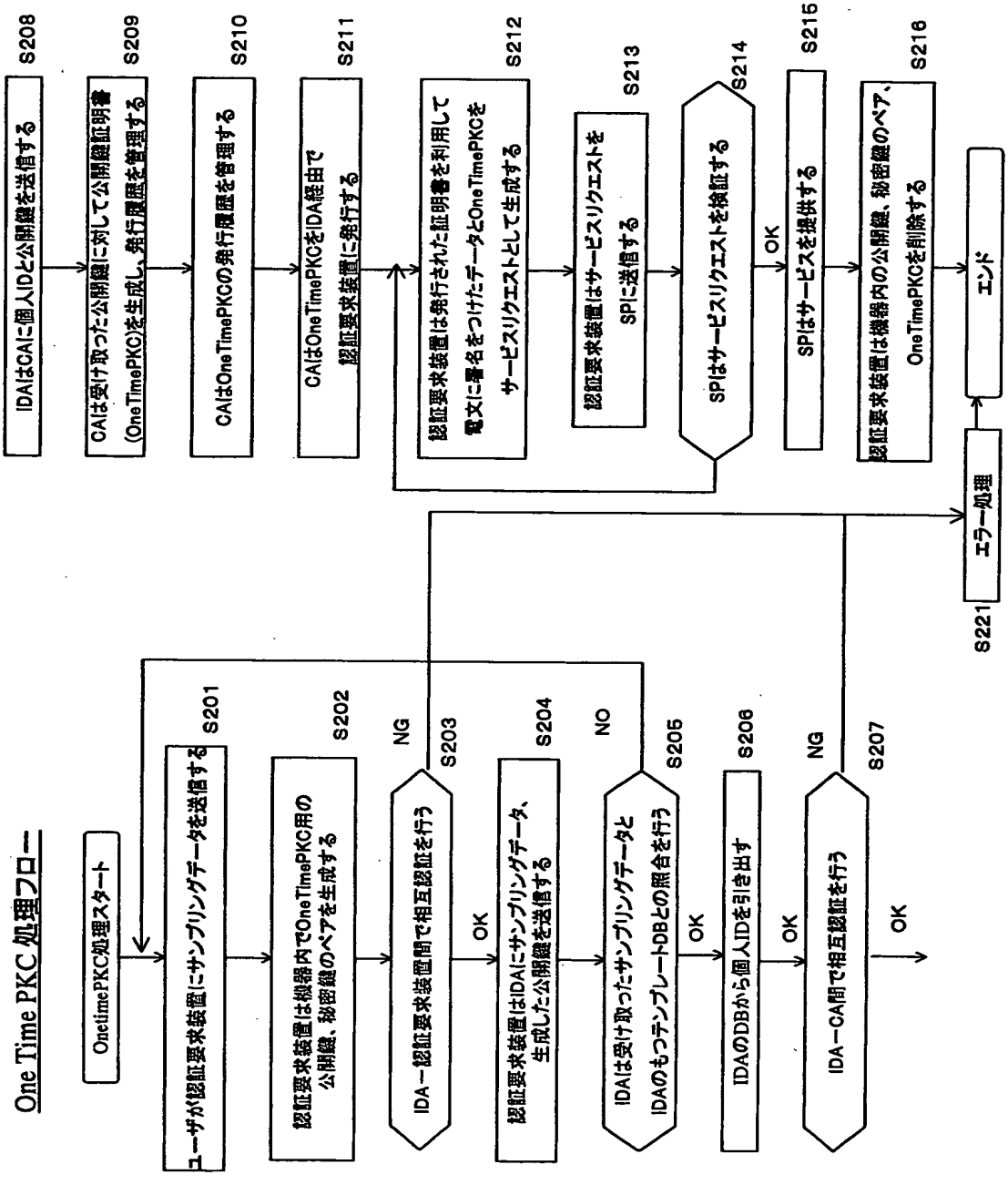
【図６５】


Device内に格納するIDC要求のフローチャート(3)
④
IDRAと接続する。
S526
相互認証＆セッション鍵を共有する。
S527
IDRAと利用者間でデータをやり取りする。
S528
IDRA・利用者間でIDC発行に必要なデータのやり取りが終わったか
No
Yes
S529
利用者に表示が必要なデータ、IDC発行の要求の結果をDownloadする。
S530
IDC発行が成功したか。
No
Yes
S531
E-④
リンク(組)情報を更新するか。
No
S532
リンク(組)情報を更新する。
S533
IDC発行要求の結果を表示する。
S534
Deviceを利用可能。
S535
E-④
IDCの発行が断られたメッセージを表示。
S536
ユーザのDevice利用確認が失敗を通知する。
S537
終了。
E-⑤
公開鍵証明書が見つからず、公開鍵証明書の新規発行が断られたメッセージを表示。
S538
ユーザのDevice利用確認の失敗を通知する。
S539
終了。

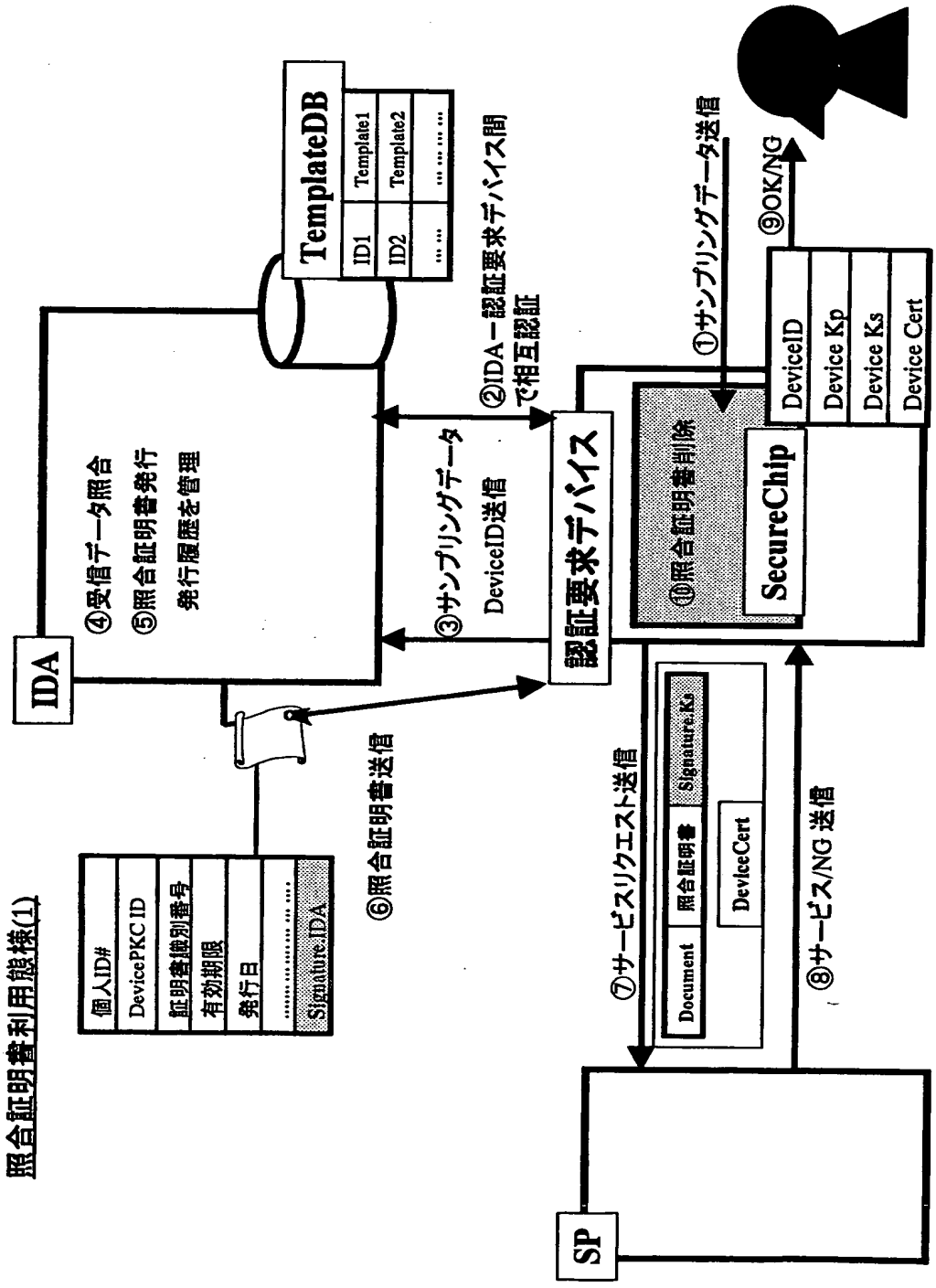
【図６６】


One Time PKC
IDA
④受信データ照合
TemplateDB
ID1
ID2
Template1
Template2
CA
⑦無審査でCert生成
ID#, OnetimePKCの発行
履歴を管理
⑤相互認証
⑥ID#、Kp送信
⑧Cert送信 (IDA経由)
ID(OnetimePKC's)
個人ID#(IDAが割り振る)
Kp
証明書識別番号
Signature,CA
認証要求デバイス
①サンプリングデータ送信
⑪OK/NG
②Kp、Ksの生成
⑫Kp,Ks,Certの削除
SecureChip
③相互認証
サンプリングデータ、Kp送信
⑨サービスリクエスト送信
Document
Signature,Ks
⑩サービス/NG 送信
SP

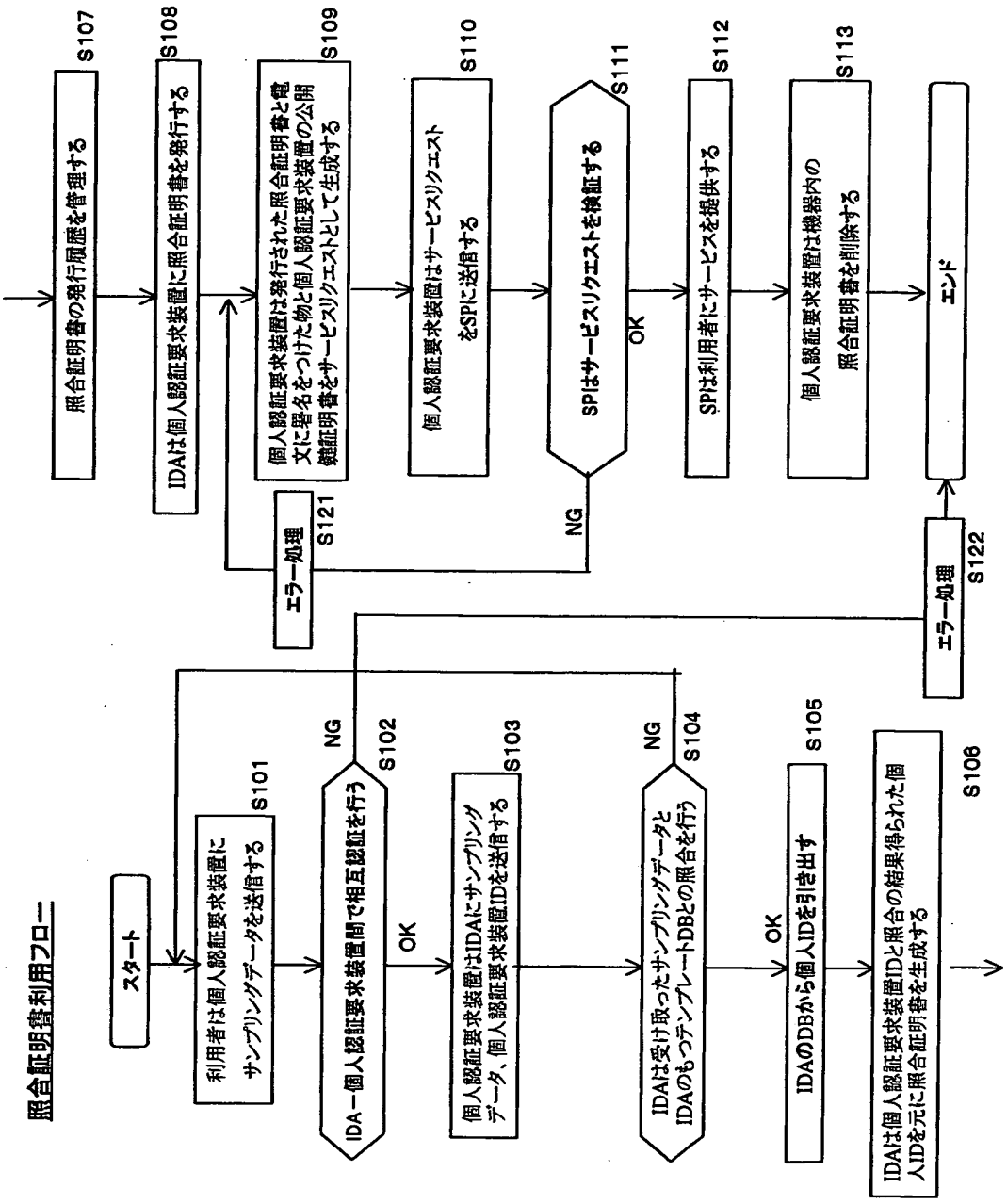
【図６７】


One Time PKC 処理フロー
OnetimePKC処理スタート
ユーザが認証要求装置にサンプリングデータを送信する
S201
認証要求装置は機器内でOneTimePKC用の公開鍵、秘密鍵のペアを生成する
S202
IDA－認証要求装置間で相互認証を行う
S203
NG
OK
認証要求装置はIDAにサンプリングデータ、生成した公開鍵を送信する
S204
IDAは受け取ったサンプリングデータとIDAのもつテンプレートDBとの照合を行う
S205
NO
OK
IDAのDBから個人IDを引き出す
S206
OK
IDA－CA間で相互認証を行う
S207
NG
OK
エラー処理
S221
IDAはCAに個人IDと公開鍵を送信する
S208
CAは受け取った公開鍵に対して公開鍵証明書(OneTimePKC)を生成し、発行履歴を管理する
S209
CAはOneTimePKCの発行履歴を管理する
S210
CAはOneTimePKCをIDA経由で認証要求装置に発行する
S211
認証要求装置は発行された証明書を利用して電文に署名をつけたデータとOneTimePKCをサービスリクエストとして生成する
S212
認証要求装置はサービスリクエストをSPに送信する
S213
SPはサービスリクエストを検証する
S214
OK
SPはサービスを提供する
S215
認証要求装置は機器内の公開鍵、秘密鍵のペア、OneTimePKCを削除する
S216
エンド

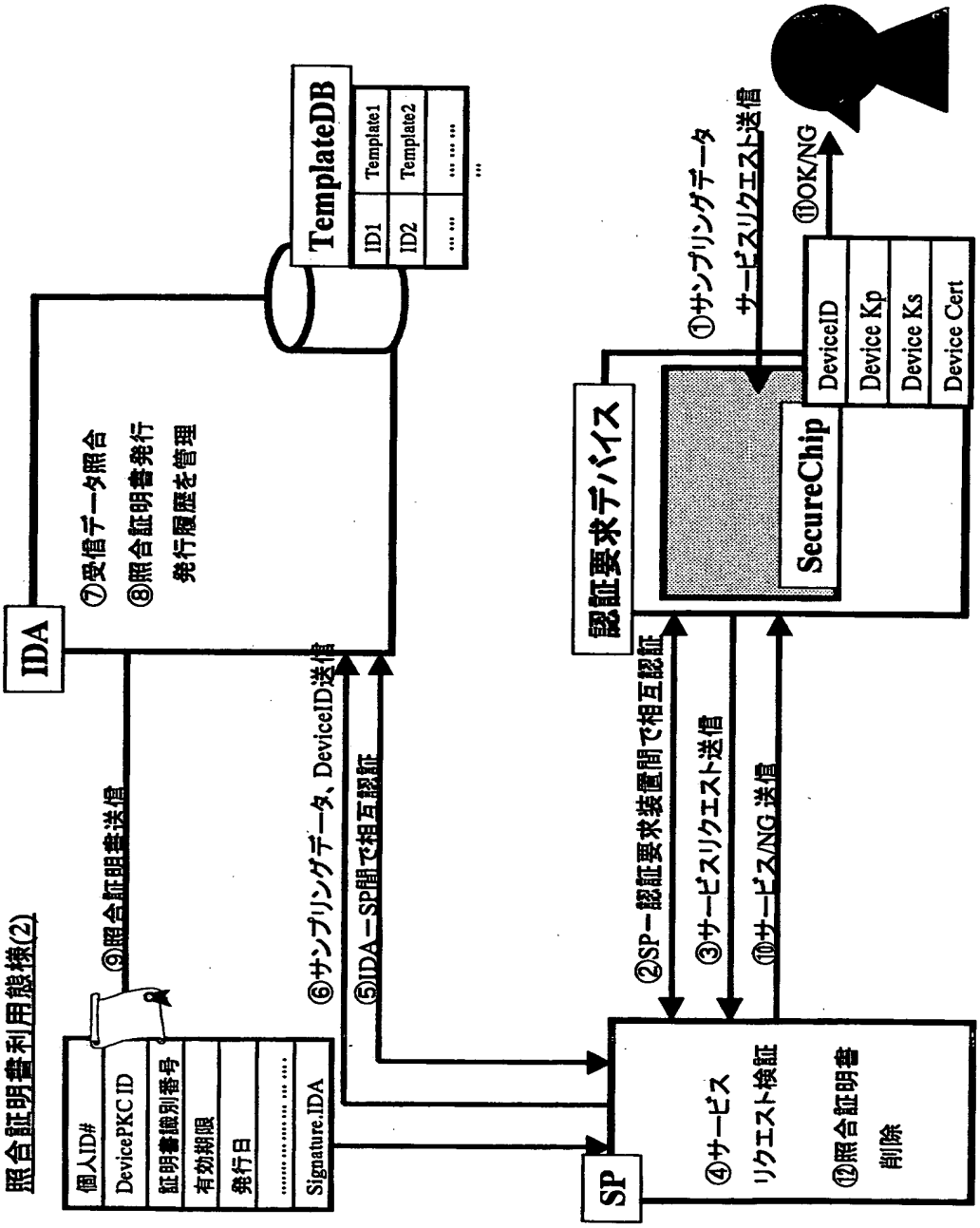
【図６８】


照合証明書利用態様(1)
個人ID#
DevicePKC ID
証明書識別番号
有効期限
発行日
Signature.IDA
⑥照合証明書送信
IDA
④受信データ照合
⑤照合証明書発行
発行履歴を管理
TemplateDB
ID1
Template1
ID2
Template2
③サンプリングデータ
DeviceID送信
②IDA－認証要求デバイス間
で相互認証
認証要求デバイス
①サンプリングデータ送信
⑨OK/NG
⑩照合証明書削除
SecureChip
DeviceID
Device Kp
Device Ks
Device Cert
⑦サービスリクエスト送信
Document
照合証明書
Signature.Ks
DeviceCert
⑧サービス/NG 送信
SP

【図６９】


照合証明書利用フロー
スタート
利用者は個人認証要求装置にサンプリングデータを送信する
S101
IDA－個人認証要求装置間で相互認証を行う
S102
NG
OK
個人認証要求装置はIDAにサンプリングデータ、個人認証要求装置IDを送信する
S103
IDAは受け取ったサンプリングデータとIDAのもつテンプレートDBとの照合を行う
S104
NG
OK
IDAのDBから個人IDを引き出す
S105
IDAは個人認証要求装置IDと照合の結果得られた個人IDを元に照合証明書を生成する
S106
エラー処理
S121
エラー処理
S122
照合証明書の発行履歴を管理する
S107
IDAは個人認証要求装置に照合証明書を発行する
S108
個人認証要求装置は発行された照合証明書と電文に署名をつけた物と個人認証要求装置の公開鍵証明書をサービスリクエストとして生成する
S109
個人認証要求装置はサービスリクエストをSPに送信する
S110
SPはサービスリクエストを検証する
S111
NG
OK
SPは利用者にサービスを提供する
S112
個人認証要求装置は機器内の照合証明書を削除する
S113
エンド

【図７０】

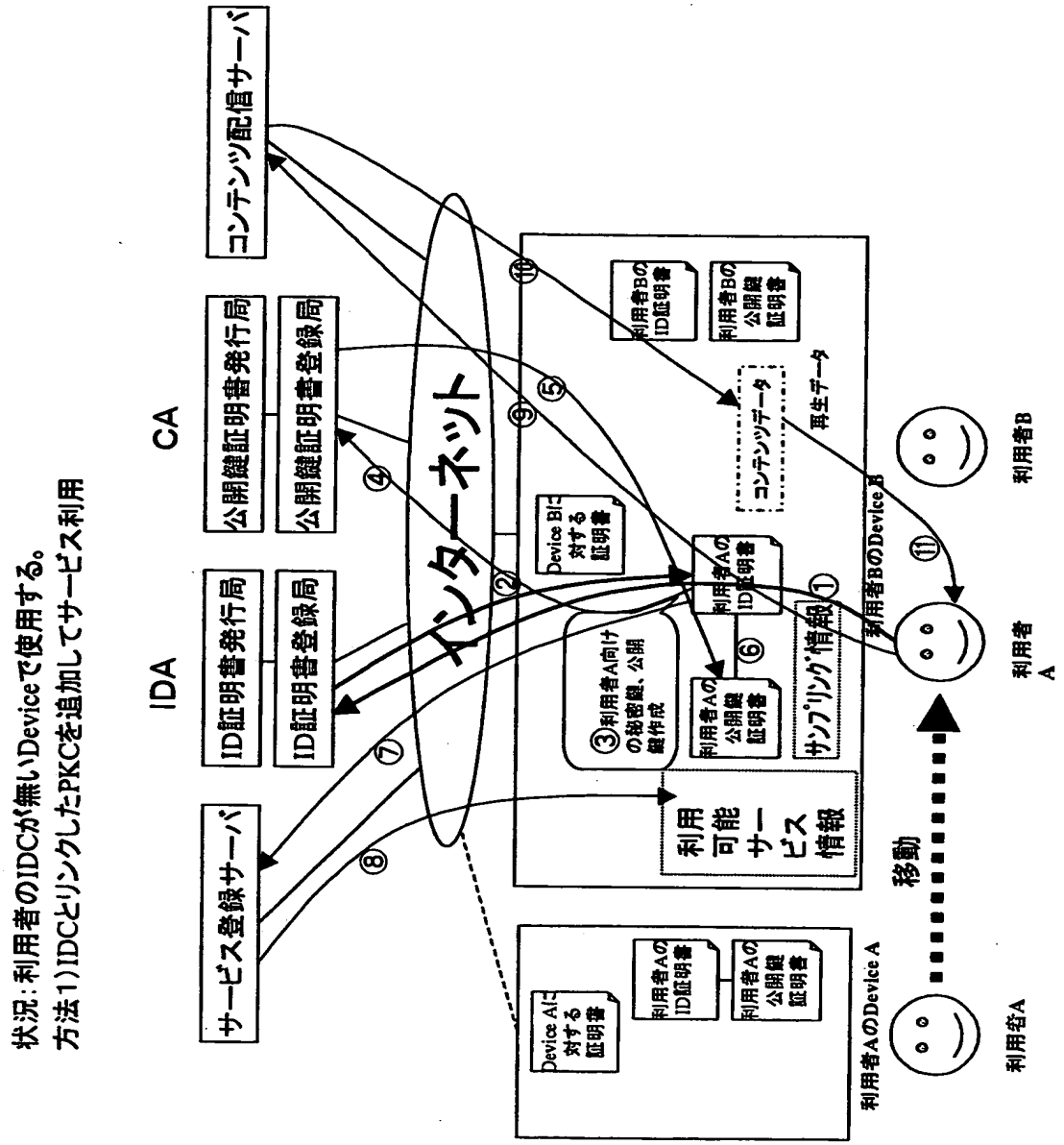

照合証明書利用態様(2)
個人ID#
DevicePKC ID
証明書識別番号
有効期限
発行日
Signature.IDA
⑨照合証明書送信
IDA
⑦受信データ照合
⑧照合証明書発行
発行履歴を管理
TemplateDB
ID1
Template1
ID2
Template2
⑥サンプリングデータ、DeviceID送信
⑤IDA－SP間で相互認証
SP
④サービス
リクエスト検証
⑫照合証明書
削除
②SP－認証要求装置間で相互認証
③サービスリクエスト送信
⑩サービスOK/NG送信
認証要求デバイス
SecureChip
DeviceID
Device Kp
Device Ks
Device Cert
①サンプリングデータ
サービスリクエスト送信
⑪OK/NG

【図７１】

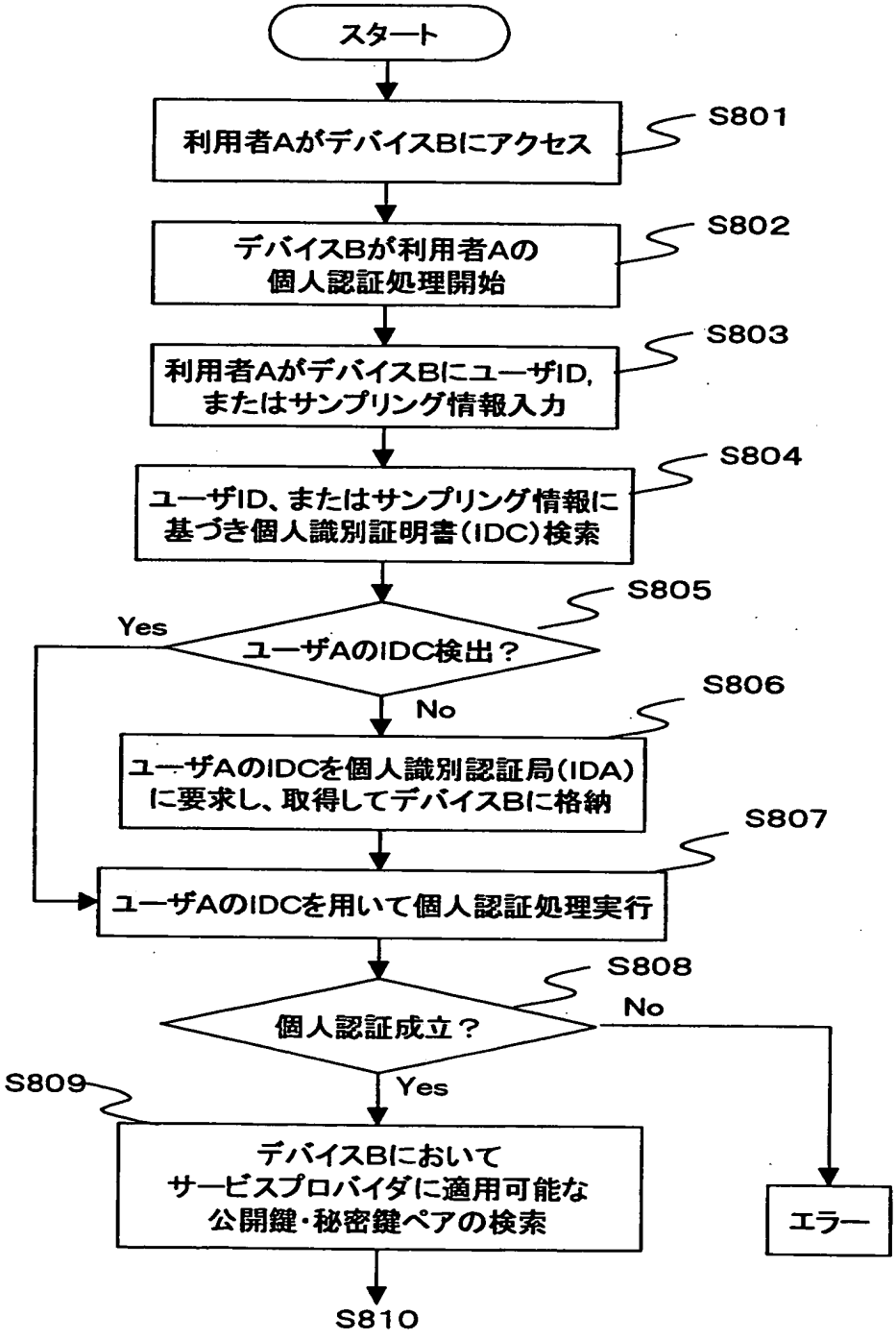
照合証明書フォーマット

	項目	説明
必須項目	Version	バージョン
	SerialNumber	認証番号
	signaturealgorithmIdentifier algorithm parameters	署名方式 アルゴリズム パラメータ
	Issuer	個人識別認証局名(Distinguished Name形式)
	Validity notBefore notAfter	有効期限 ・ 開始日時 ・ 終了日時
	subject	被認証者名(DN形式)
	subjectIDAInfo subjectIDAserialNumber subjectIDAUniqueID	被認証者の個人識別証明書情報 ・ 被認証者の個人識別証明書の認証番号 ・ 被認証者の個人識別証明書の被認証者固有ID
	subjectPKCinfo subjectPKCserialNumber subjectPKCUniqueID	被認証者の公開鍵証明書情報 ・ 被認証者の公開鍵証明書の認証番号 ・ 被認証者の公開鍵証明書の被認証者固有ID
必	IDASignature	IDAの署名

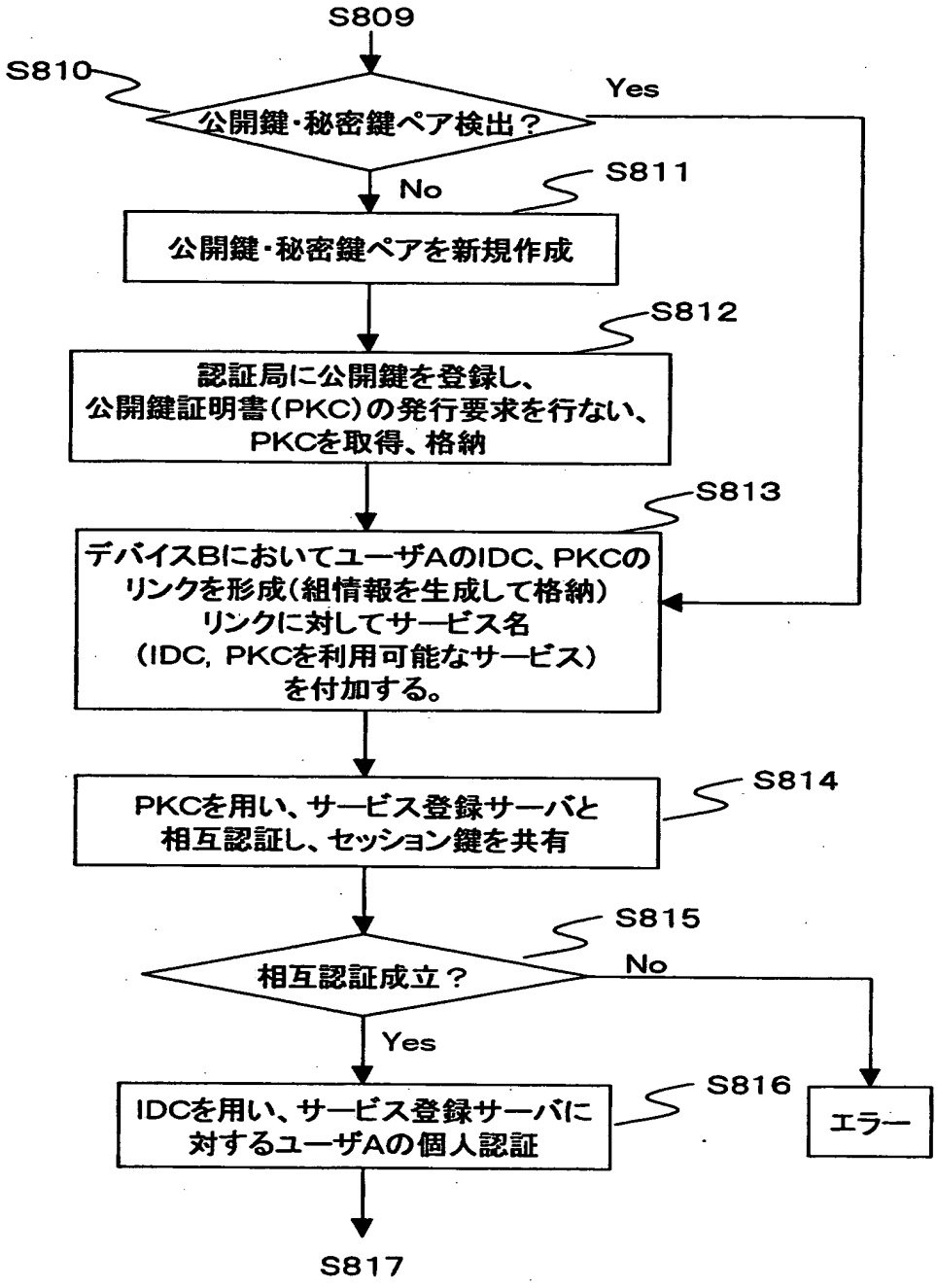
【図７２】


状況：利用者のIDCが無いDeviceで使用する。
方法1）IDCとリンクしたPKCを追加してサービス利用
IDA
CA
ID証明書発行局
ID証明書登録局
公開鍵証明書発行局
公開鍵証明書登録局
コンテンツ配信サーバ
サービス登録サーバ
インターネット
Device AIに対する証明書
利用者AのID証明書
利用者Aの公開鍵証明書
利用者AのDevice A
利用者A
移動
利用者B
利用者BのDevice B
Device BIに対する証明書
利用者BのID証明書
利用者Bの公開鍵証明書
コンテンツデータ
再生データ
利用者Aの公開鍵証明書
サンプリング情報
③利用者A向けの秘密鍵、公開鍵作成
利用可能サービス情報
①
②
④
⑤
⑥
⑦
⑧
⑨
⑩
⑪

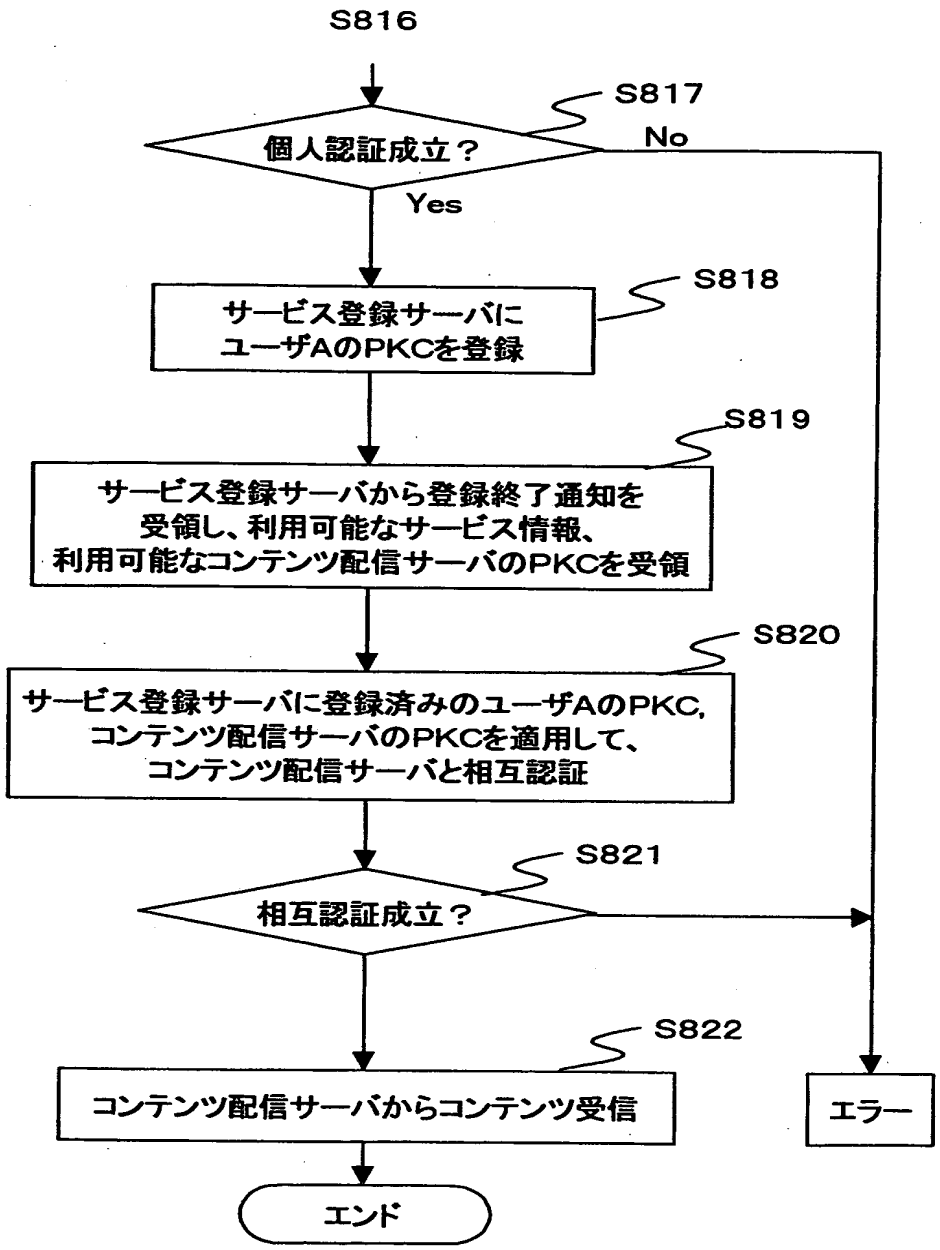
【図７３】


スタート
利用者Aがデバイスbにアクセス
S801
デバイスBが利用者Aの
個人認証処理開始
S802
利用者Aがデバイスbにユーザid,
またはサンプリング情報入力
S803
ユーザID、またはサンプリング情報に
基づき個人識別証明書(IDC)検索
S804
S805
Yes
ユーザAのIDC検出？
No
S806
ユーザAのIDCを個人識別認証局(IDA)
に要求し、取得してデバイスBに格納
S807
ユーザAのIDCを用いて個人認証処理実行
S808
個人認証成立？
No
Yes
S809
デバイスBにおいて
サービスプロバイダに適用可能な
公開鍵・秘密鍵ペアの検索
エラー
S810

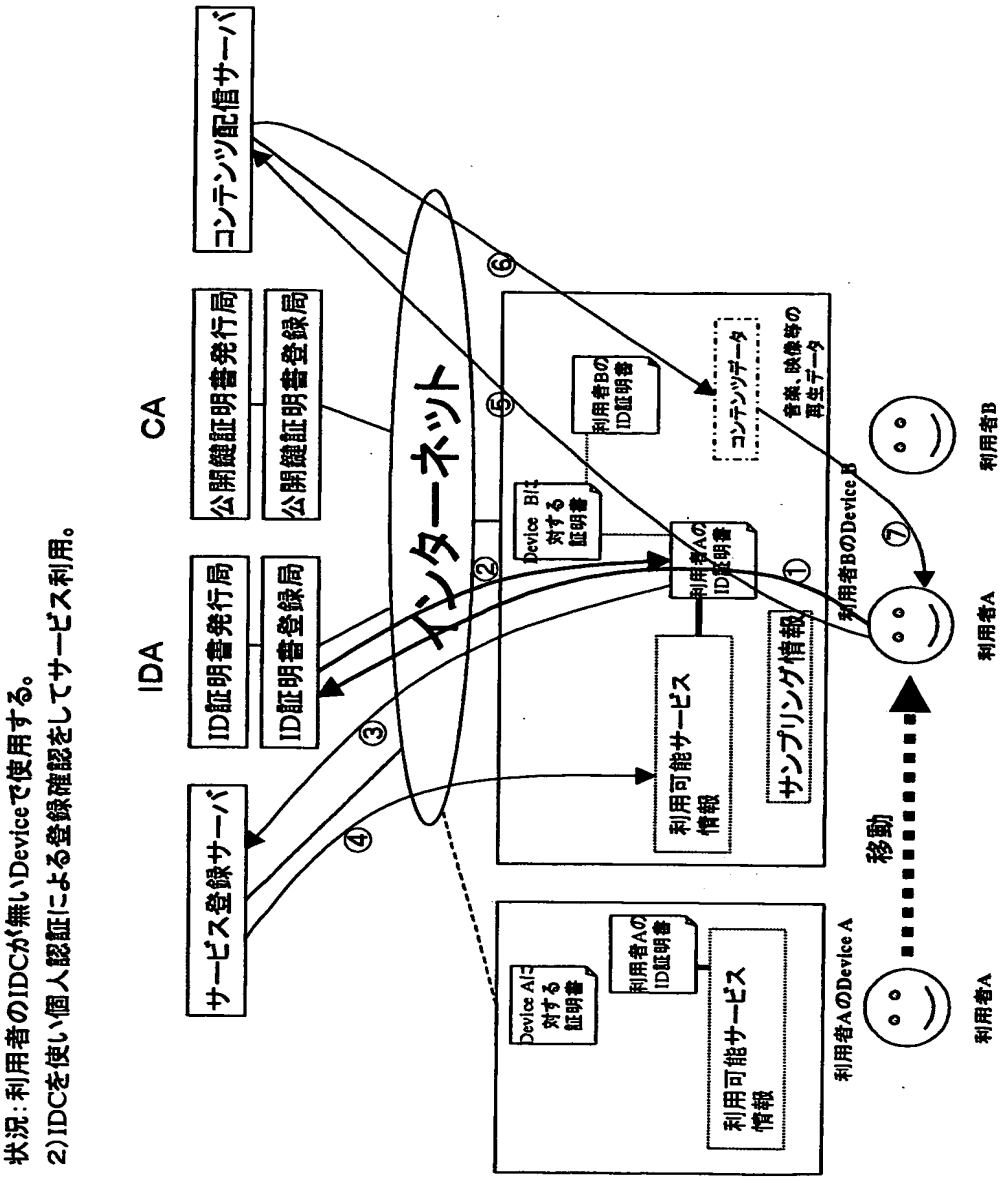
【図７４】


S809
S810
公開鍵・秘密鍵ペア検出？
Yes
No
S811
公開鍵・秘密鍵ペアを新規作成
S812
認証局に公開鍵を登録し、
公開鍵証明書(PKC)の発行要求を行ない、
PKCを取得、格納
S813
デバイスBにおいてユーザAのIDC、PKCの
リンクを形成(組情報を生成して格納)
リンクに対してサービス名
(IDC, PKCを利用可能なサービス)
を付加する。
PKCを用い、サービス登録サーバと
相互認証し、セッション鍵を共有
S814
S815
相互認証成立？
No
Yes
IDCを用い、サービス登録サーバに
対するユーザAの個人認証
S816
エラー
S817

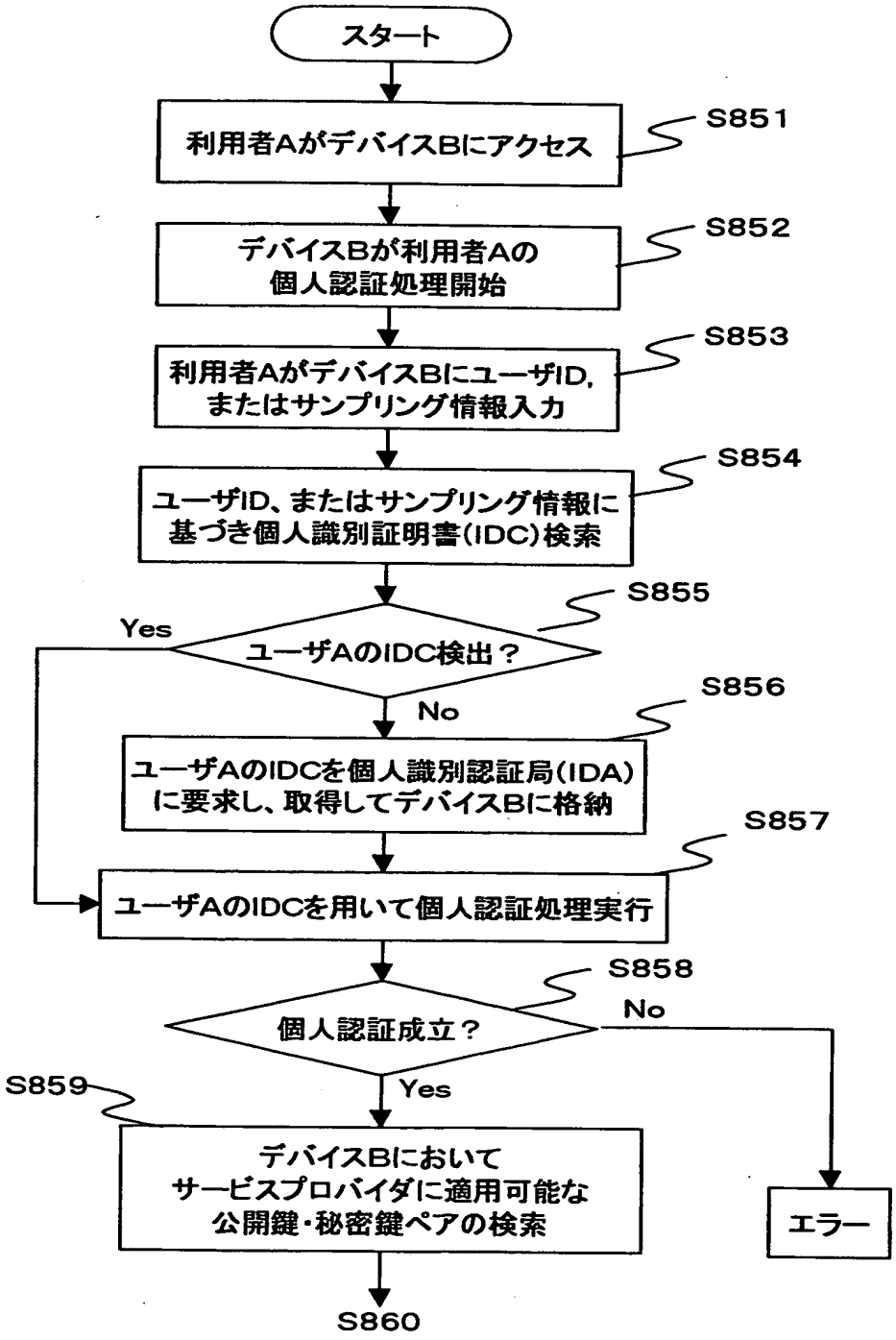
【図７５】


S816
S817
個人認証成立？
No
Yes
S818
サービス登録サーバに
ユーザAのPKCを登録
S819
サービス登録サーバから登録終了通知を
受領し、利用可能なサービス情報、
利用可能なコンテンツ配信サーバのPKCを受領
S820
サービス登録サーバに登録済みのユーザAのPKC,
コンテンツ配信サーバのPKCを適用して、
コンテンツ配信サーバと相互認証
S821
相互認証成立？
S822
コンテンツ配信サーバからコンテンツ受信
エラー
エンド

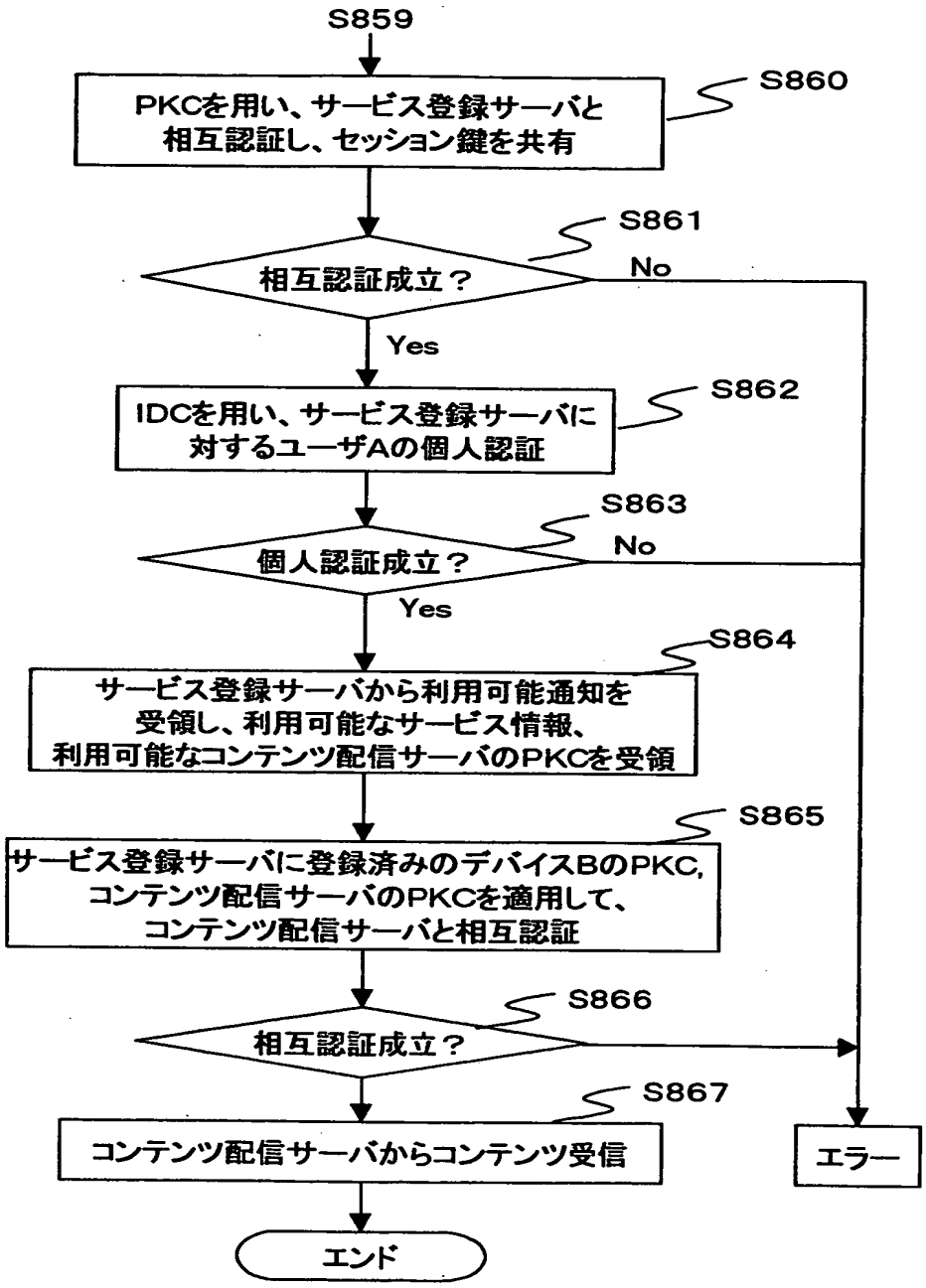
【図７６】


状況：利用者のIDCが無いDeviceで使用する。
2）IDCを使い個人認証による登録確認をしてサービス利用。
IDA
CA
ID証明書発行局
ID証明書登録局
公開鍵証明書発行局
公開鍵証明書登録局
サービス登録サーバ
コンテンツ配信サーバ
インターネット
利用可能サービス情報
サンプリング情報
コンテンツデータ
音楽、映像等の再生データ
利用者AのID証明書
利用者BのID証明書
Device Aに対する証明書
Device Bに対する証明書
利用者AのDevice A
利用者BのDevice B
移動
利用者A
利用者B

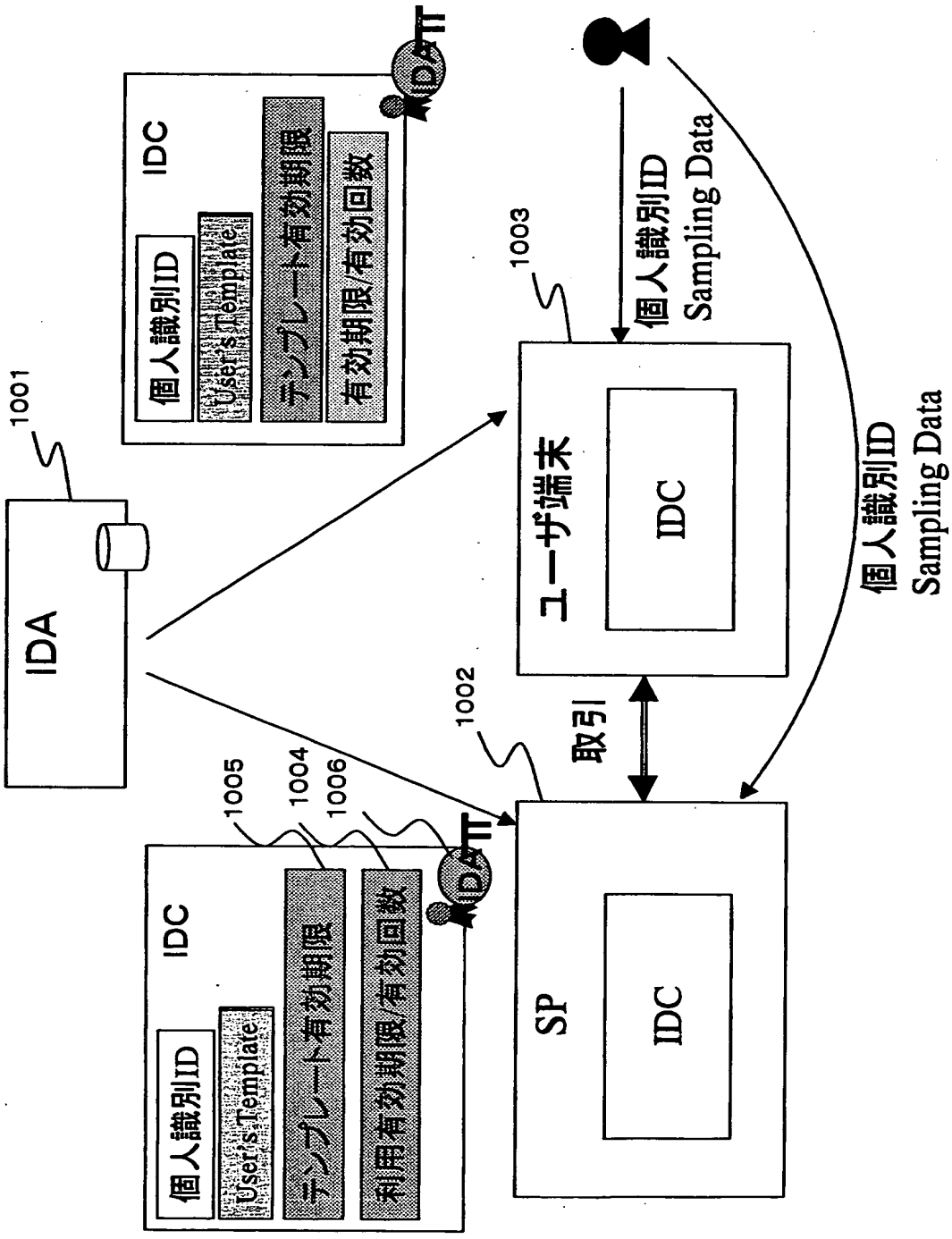
【図７７】


スタート
利用者Aがデバイスbにアクセス
S851
デバイスBが利用者Aの
個人認証処理開始
S852
利用者Aがデバイスbにユーザid,
またはサンプリング情報入力
S853
ユーザID、またはサンプリング情報に
基づき個人識別証明書(IDC)検索
S854
S855
Yes
ユーザAのIDC検出？
No
S856
ユーザAのIDCを個人識別認証局(IDA)
に要求し、取得してデバイスBに格納
S857
ユーザAのIDCを用いて個人認証処理実行
S858
個人認証成立？
No
Yes
S859
デバイスBにおいて
サービスプロバイダに適用可能な
公開鍵・秘密鍵ペアの検索
エラー
S860

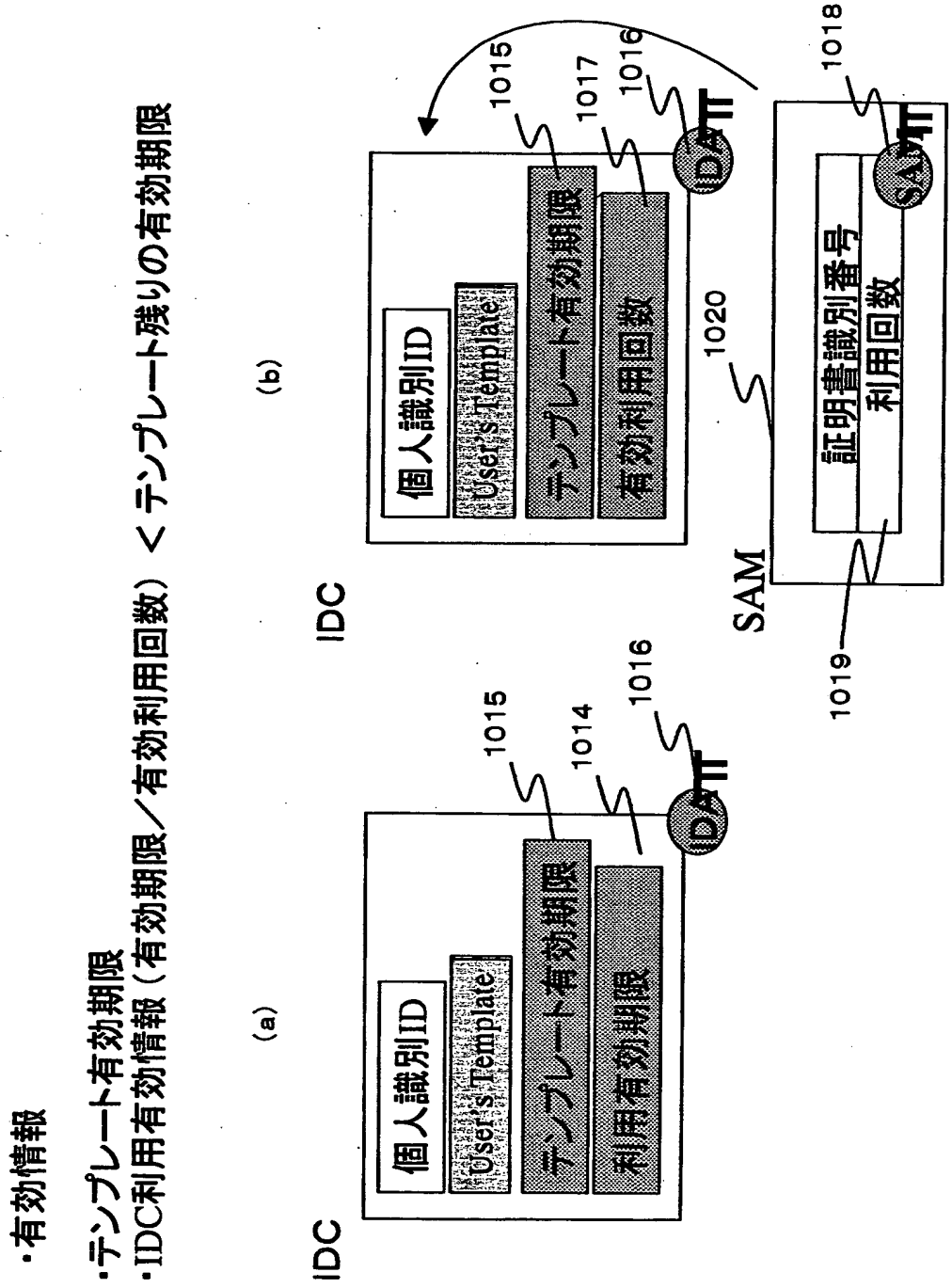
【図７８】


S859
PKCを用い、サービス登録サーバと
相互認証し、セッション鍵を共有
S860
S861
相互認証成立？
No
Yes
IDCを用い、サービス登録サーバに
対するユーザAの個人認証
S862
S863
個人認証成立？
No
Yes
S864
サービス登録サーバから利用可能通知を
受領し、利用可能なサービス情報、
利用可能なコンテンツ配信サーバのPKCを受領
S865
サービス登録サーバに登録済みのデバイスBのPKC,
コンテンツ配信サーバのPKCを適用して、
コンテンツ配信サーバと相互認証
S866
相互認証成立？
S867
コンテンツ配信サーバからコンテンツ受信
エラー
エンド

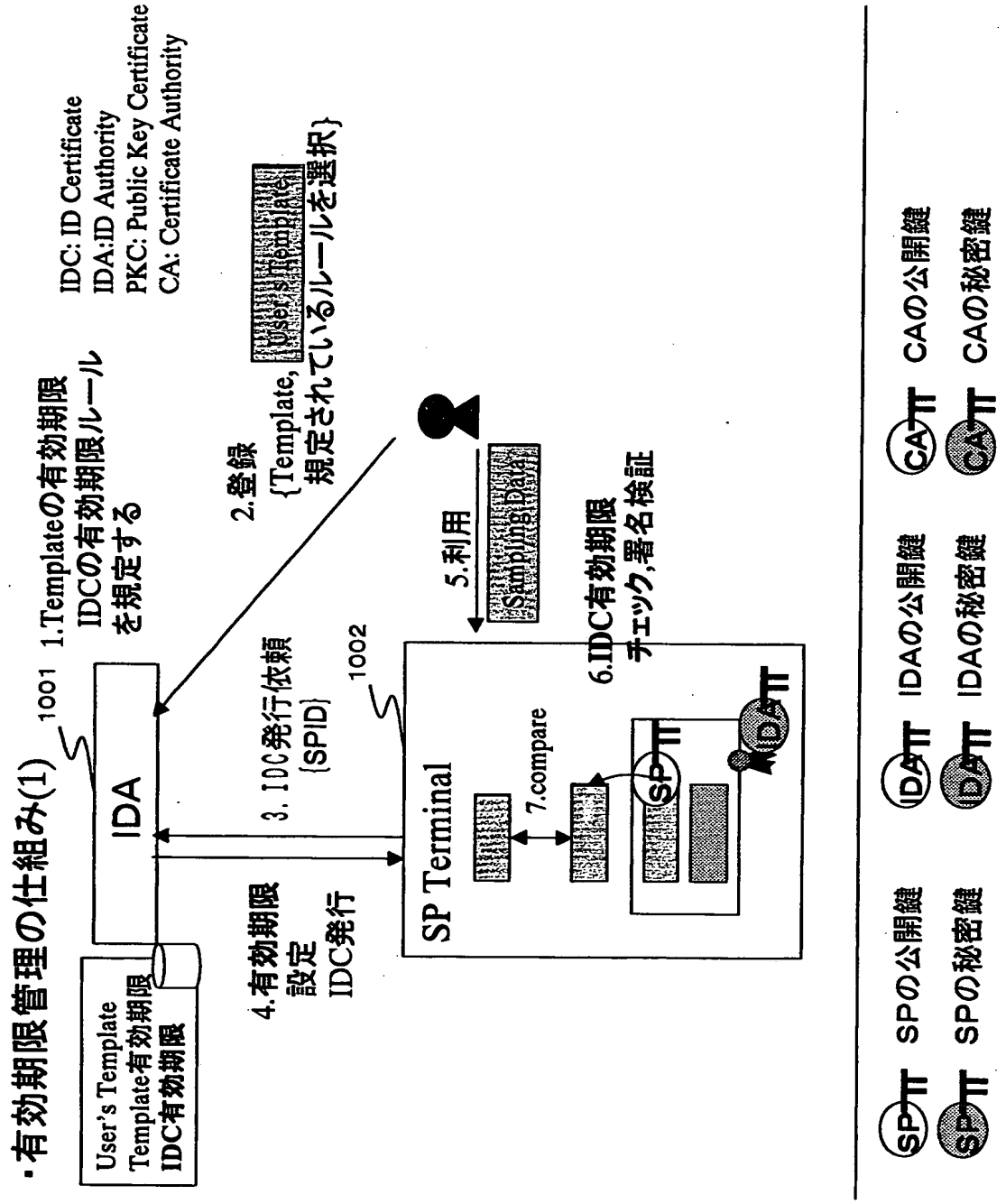
【図７９】


IDA
1001
IDC
個人識別ID
User's Template
テンプレート有効期限
有効期限/有効回数
DATT
1003
ユーザ端末
IDC
個人識別ID
Sampling Data
個人識別ID
Sampling Data
1002
取引
SP
IDC
1005
1004
1006
IDC
個人識別ID
User's Template
テンプレート有効期限
利用有効期限/有効回数
DATT

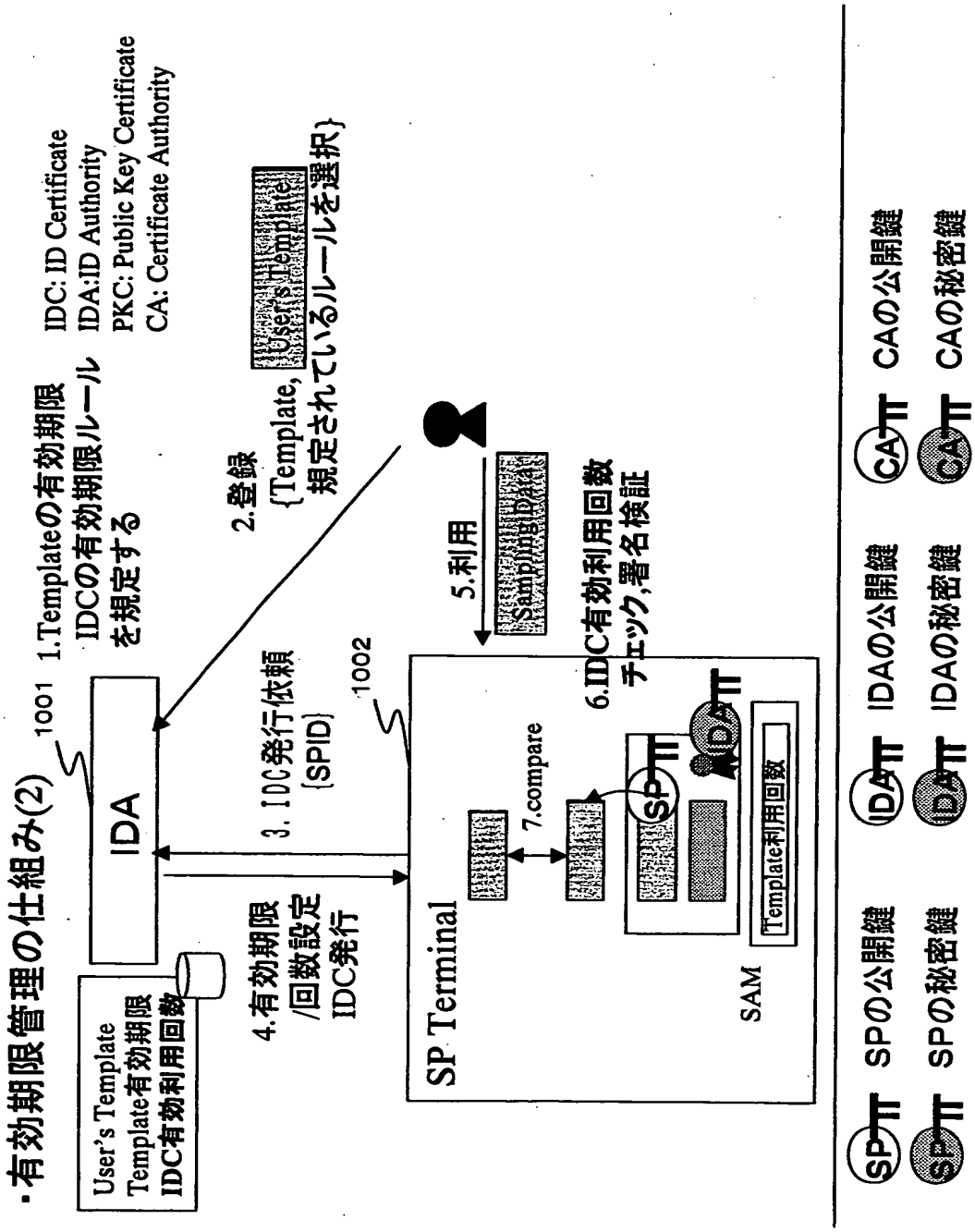
【図８０】


・有効情報
・テンプレート有効期限
・IDC利用有効情報（有効期限／有効利用回数）＜テンプレート残りの有効期限
(a)
IDC
個人識別ID
User's Template
テンプレート有効期限
利用有効期限
IDATT
1015
1014
1016
(b)
IDC
個人識別ID
User's Template
テンプレート有効期限
有効利用回数
IDATT
1015
1017
1016
1020
SAM
証明書識別番号
利用回数
SATT
1018
1019

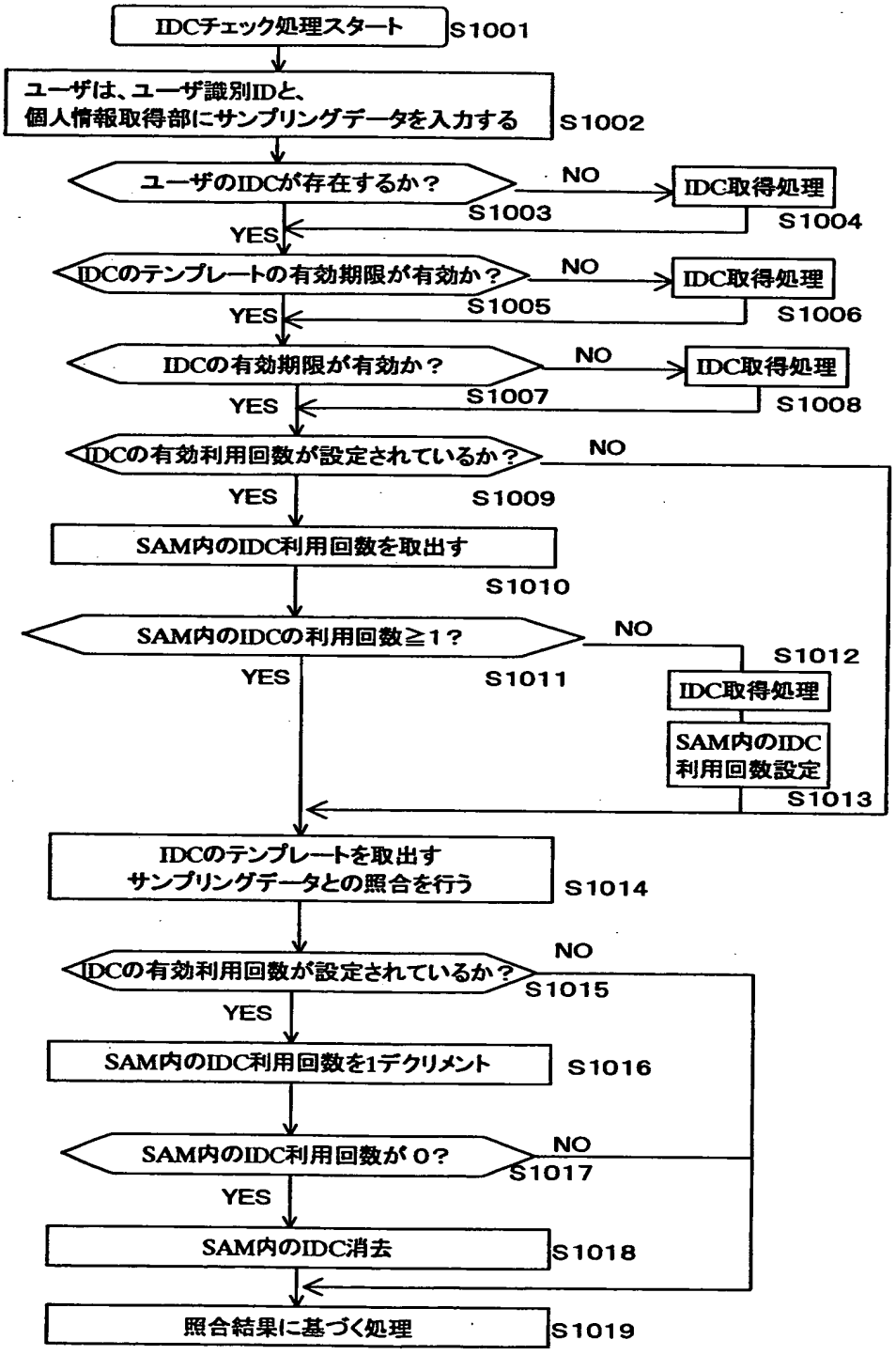
【図８１】


・有効期限管理の仕組み(1)
1001
IDA
User's Template
Template有効期限
IDC有効期限
1.Templateの有効期限
IDCの有効期限ルール
を規定する
IDC: ID Certificate
IDA:ID Authority
PKC: Public Key Certificate
CA: Certificate Authority
2.登録
{Template, User's Template
規定されているルールを選択}
3. IDC発行依頼
{SPID}
4.有効期限
設定
IDC発行
1002
SP Terminal
5.利用
Sampling Data
7.compare
6.IDC有効期限
チェック,署名検証
SP
IDA
SPの公開鍵
SPの秘密鍵
IDAの公開鍵
IDAの秘密鍵
CA
CAの公開鍵
CAの秘密鍵

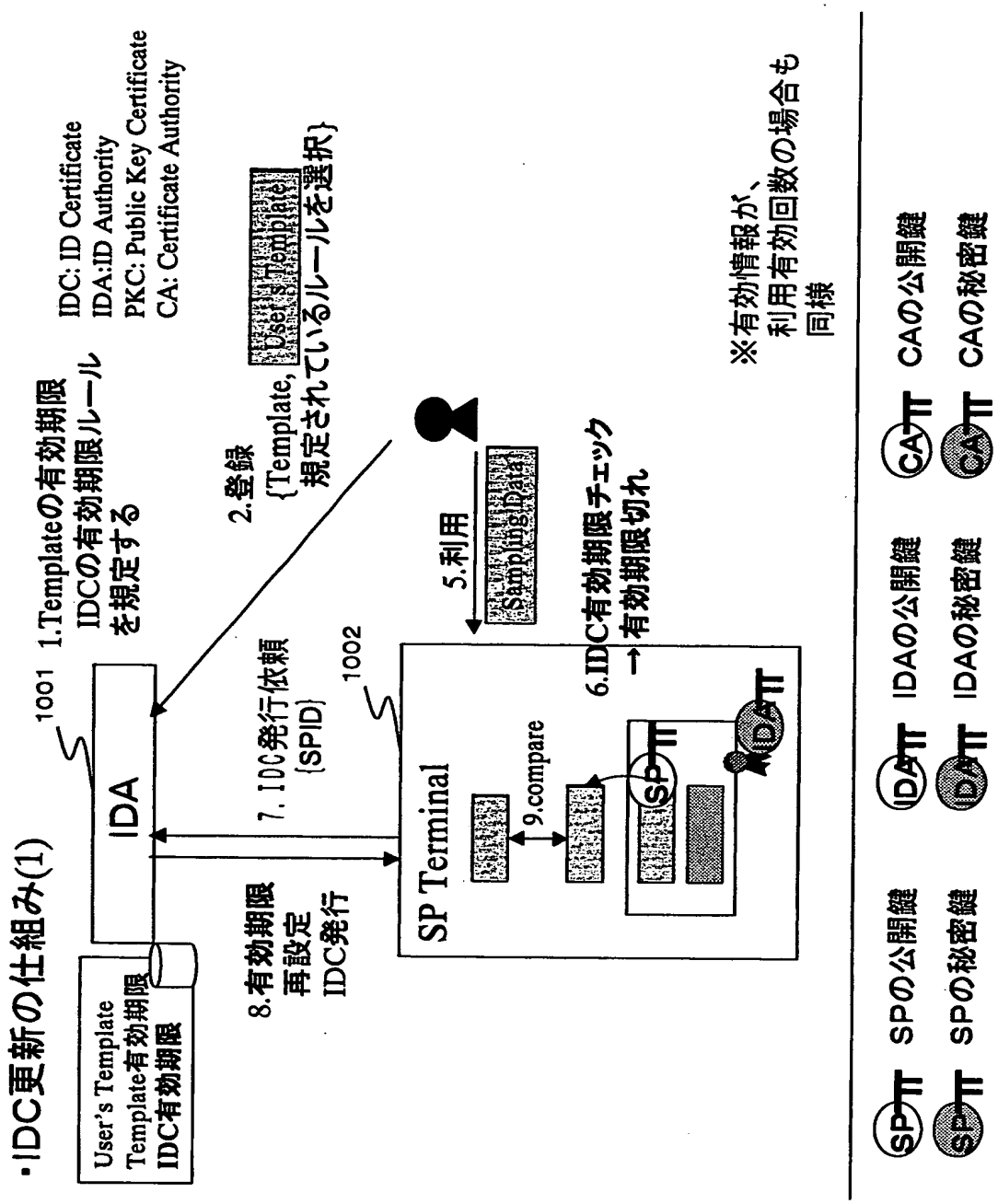
【図８２】


・有効期限管理の仕組み(2)
1001
IDA
1.Templateの有効期限
IDCの有効期限ルール
を規定する
IDC: ID Certificate
IDA:ID Authority
PKC: Public Key Certificate
CA: Certificate Authority
2.登録
{Template, User's Template
規定されているルールを選択}
3. IDC発行依頼
{SPID}
4.有効期限
/回数設定
IDC発行
User's Template
Template有効期限
IDC有効利用回数
1002
SP Terminal
5.利用
Sampling DATA
6.IDC有効利用回数
チェック,署名検証
7.compare
SAM
Template利用回数
SPの公開鍵
SPの秘密鍵
IDAの公開鍵
IDAの秘密鍵
CAの公開鍵
CAの秘密鍵

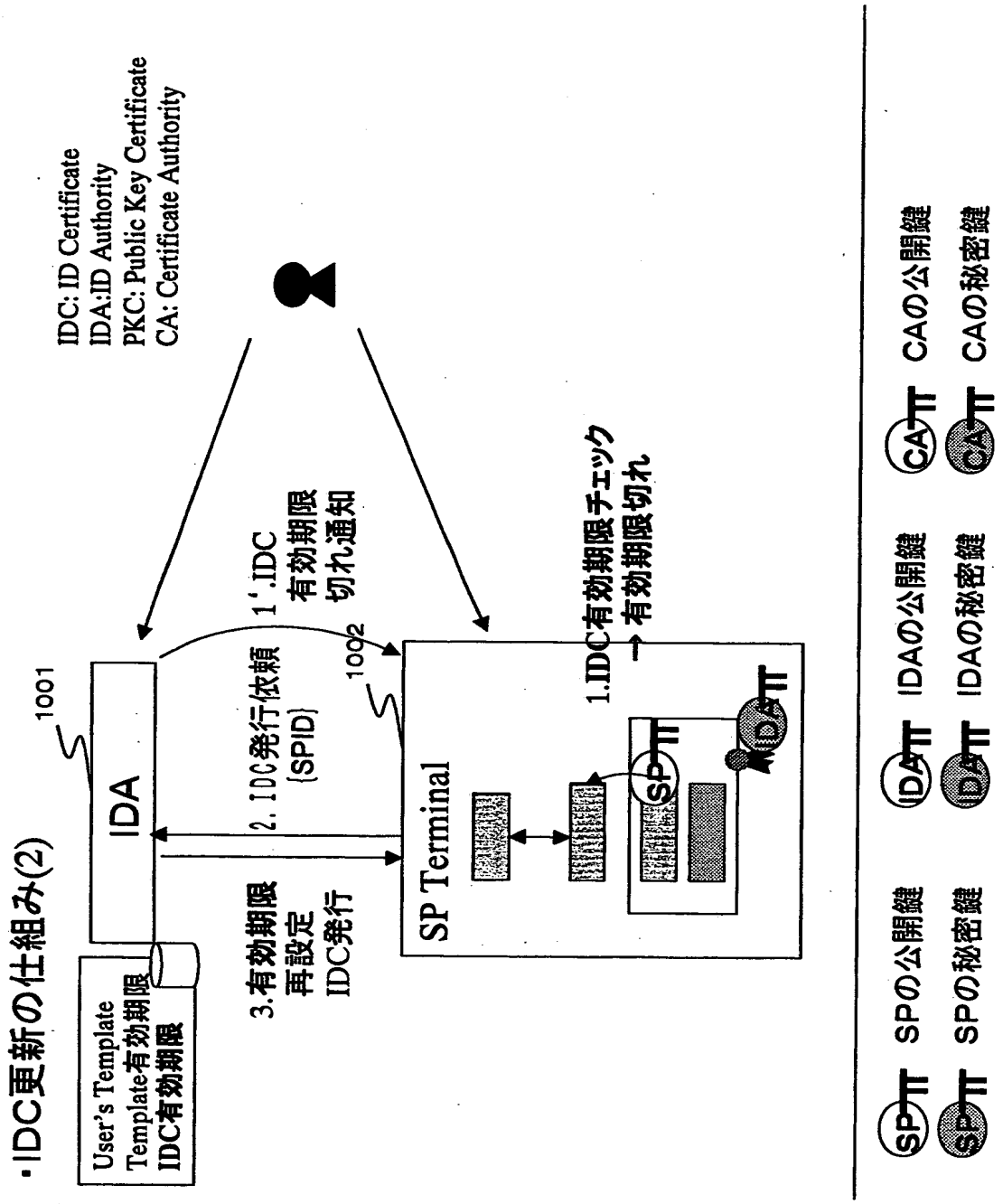
【図８３】


IDCチェック処理スタート
S1001
ユーザは、ユーザ識別IDと、
個人情報取得部にサンプリングデータを入力する
S1002
ユーザのIDCが存在するか？
NO
IDC取得処理
S1003
S1004
YES
IDCのテンプレートの有効期限が有効か？
NO
IDC取得処理
S1005
S1006
YES
IDCの有効期限が有効か？
NO
IDC取得処理
S1007
S1008
YES
IDCの有効利用回数が設定されているか？
NO
YES
S1009
SAM内のIDC利用回数を取出す
S1010
SAM内のIDCの利用回数≧1？
NO
S1012
YES
S1011
IDC取得処理
SAM内のIDC
利用回数設定
S1013
IDCのテンプレートを取出す
サンプリングデータとの照合を行う
S1014
IDCの有効利用回数が設定されているか？
NO
S1015
YES
SAM内のIDC利用回数を1デクリメント
S1016
SAM内のIDC利用回数が０？
NO
S1017
YES
SAM内のIDC消去
S1018
照合結果に基づく処理
S1019

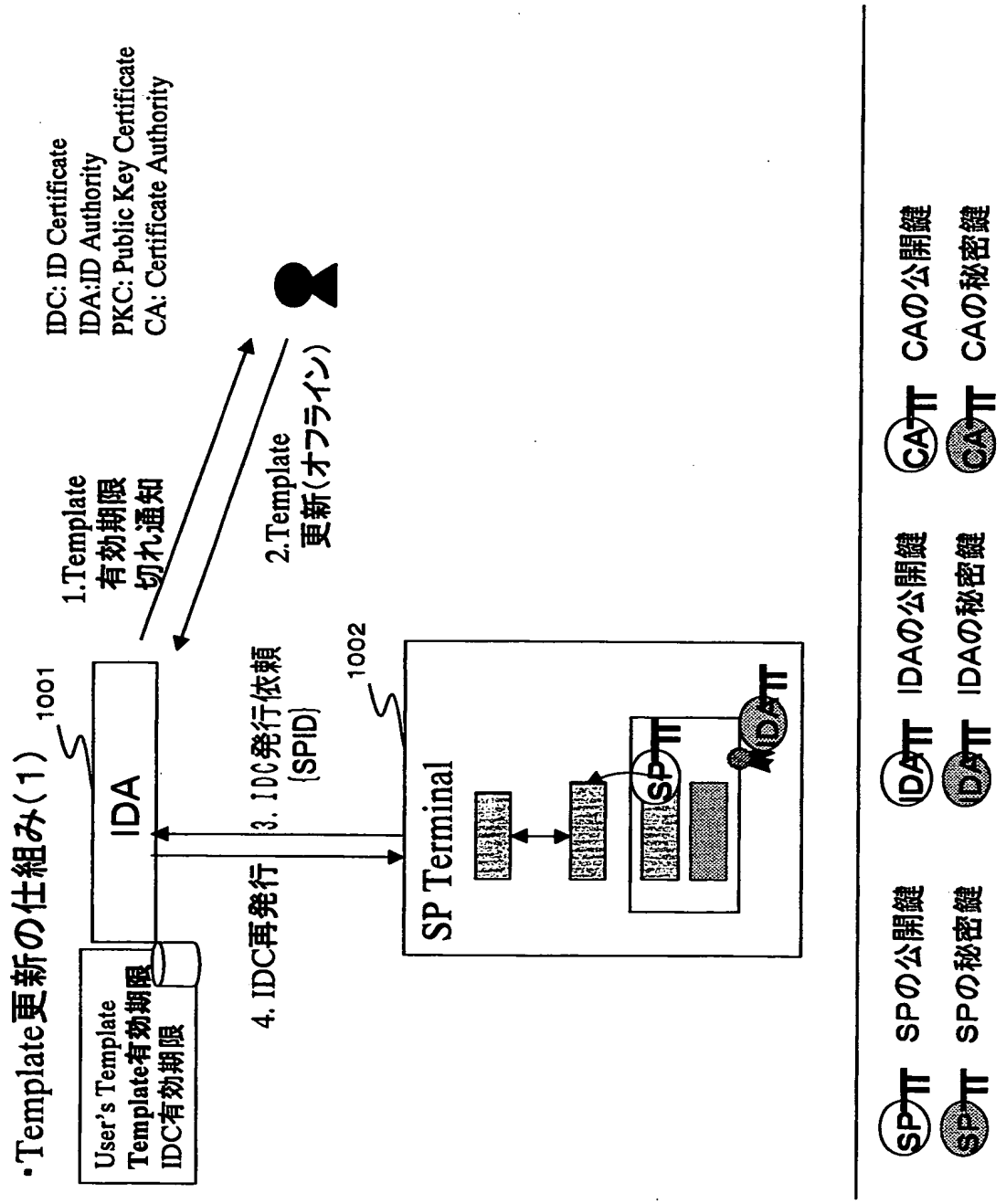
【図８４】


・IDC更新の仕組み(1)
IDA
1001
User's Template
Template有効期限
IDC有効期限
1.Templateの有効期限
IDCの有効期限ルール
を規定する
IDC: ID Certificate
IDA:ID Authority
PKC: Public Key Certificate
CA: Certificate Authority
2.登録
{Template, User's Template
規定されているルールを選択}
7. IDC発行依頼
{SPID}
8.有効期限
再設定
IDC発行
1002
SP Terminal
5.利用
Sample.IData
9.compare
6.IDC有効期限チェック
→有効期限切れ
※有効情報が、
利用有効回数の場合も
同様
SPの公開鍵
SPの秘密鍵
IDAの公開鍵
IDAの秘密鍵
CAの公開鍵
CAの秘密鍵

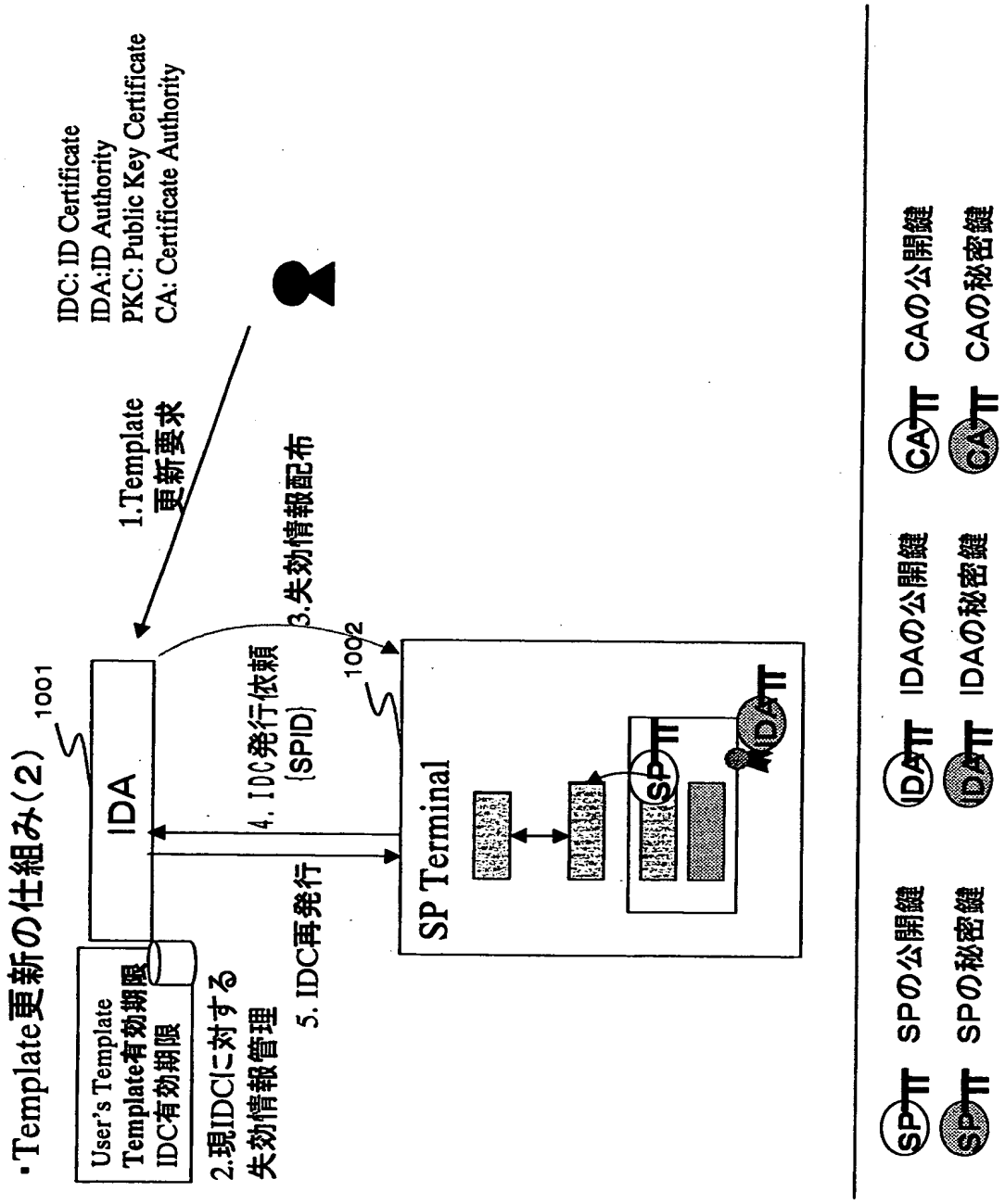
【図８５】


IDC: ID Certificate
IDA:ID Authority
PKC: Public Key Certificate
CA: Certificate Authority
・IDC更新の仕組み(2)
IDA
1001
User's Template
Template有効期限
IDC有効期限
2. IDC発行依頼
(SPID)
3.有効期限
再設定
IDC発行
1'.IDC
有効期限
切れ通知
1002
SP Terminal
1.IDC有効期限チェック
→有効期限切れ
SP
IDA
SPの公開鍵
SPの秘密鍵
IDAの公開鍵
IDAの秘密鍵
CAの公開鍵
CAの秘密鍵

【図８６】


IDC: ID Certificate
IDA:ID Authority
PKC: Public Key Certificate
CA: Certificate Authority
・Template更新の仕組み(1)
1001
IDA
User's Template
Template有効期限
IDC有効期限
1.Template
有効期限
切れ通知
2.Template
更新(オフライン)
3. IDC発行依頼
(SPID)
4. IDC再発行
1002
SP Terminal
SP
IDA
SPの公開鍵
SPの秘密鍵
IDAの公開鍵
IDAの秘密鍵
CAの公開鍵
CAの秘密鍵

【図８７】


IDC: ID Certificate
IDA:ID Authority
PKC: Public Key Certificate
CA: Certificate Authority
・Template更新の仕組み(2)
1001
IDA
User's Template
Template有効期限
IDC有効期限
1.Template
更新要求
2.現IDCに対する
失効情報管理
3.失効情報配布
4. IDC発行依頼
(SPID)
5. IDC再発行
1002
SP Terminal
SP
IDA
SPの公開鍵
SPの秘密鍵
IDAの公開鍵
IDAの秘密鍵
CAの公開鍵
CAの秘密鍵

【書類名】　要約書

【要約】

【課題】　個人識別データであるテンプレートを格納した個人識別証明書と公開鍵証明書とを関連付けて処理の効率化を実現したシステムを提供する。

【解決手段】　個人識別データであるテンプレートを格納し、個人識別認証局が生成する個人識別証明書と、公開鍵を格納した公開鍵証明書との間でリンクを形成し、１つの証明書に基づいて他の証明書を特定可能とした。本構成により、例えば個人識別証明書に格納したテンプレートの暗号処理鍵の特定や、サービスプロバイダとの取り引き時に適用する個人識別証明書と公開鍵証明書との組を迅速に取得することが可能となり、各種の処理において効率化が実現される。

【選択図】　図４７

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社